CABLETRON SYSTEMS

REMOTE ACCESS MODULE

Smart SWITCH

USER'S GUIDE

Release 7.2

Cabletron Systems
(603) 332-9400 phone
(603) 337-3075 fax
support@ctron.com

Only qualified personnel should perform installation procedures.

NOTICE

You may post this document on a network server for public use as long as no modifications are made to the document.

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

©Copyright 1998 by Cabletron Systems, Inc. All rights reserved.

Cabletron Systems, Inc.
P.O. Box 5005
Rochester, NH 03866-5005

Order Number: 9032490

VIRUS DISCLAIMER

Cabletron Systems has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Cabletron Systems makes no representations or warranties to the effect that the Licensed Software is virus-free.

Copyright © July 1997, by Cabletron Systems, Inc. All rights reserved.

TRADEMARKS

Cabletron Systems, CyberSWITCH, MMAC-Plus, SmartSWITCH, SPECTRUM, and SecureFast Virtual Remote Access Manager are trademarks of Cabletron Systems, Inc.

All other product names mentioned in this manual are trademarks or registered trademarks of their respective companies.

COPYRIGHTS

All of the code for this product is copyrighted by Cabletron Systems, Inc.

© Copyright 1991-1997 Cabletron Systems, Inc. All rights reserved. Printed in the United States of America.

Portions of the code for this product are copyrighted by the following corporations:

Epilogue Technology Corporation
Copyright 1991-1993 by Epilogue Technology Corporation. All rights reserved.

Livingston Enterprises, Inc.
Copyright 1992 Livingston Enterprises, Inc.

Security Dynamics Technologies Inc.
Copyright 1995 by Security Dynamics Technologies Inc. All rights reserved.

Stac Electronics
Stac Electronics 1993, including one or more U.S. Patents No. 4701745, 5016009, 5126739 and 5146221 and other pending patents.

Telenetworks
Copyright 1991, 92, 93 by Telenetworks. All rights reserved.

FCC NOTICE

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

WARNING: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

DOC NOTICE

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

VCCI NOTICE

This is a Class 1 product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、第一種情報装置（商工業地域において使用されるべき情報装置）で商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（VCCI）基準に適合しております。
従って、住宅地域またはその隣接した地域で使用すると、ラジオ、テレビジョン受信機等に受信障害を与えることがあります。
取扱説明書に従って正しい取り扱いをして下さい。

CABLETRON SYSTEMS, INC. PROGRAM LICENSE AGREEMENT

IMPORTANT: Before utilizing this product, carefully read this License Agreement.

This document is an agreement between you, the end user, and Cabletron Systems, Inc. ("Cabletron") that sets forth your rights and obligations with respect to the Cabletron software program (the "Program") contained in this package. The Program may be contained in firmware, chips or other media. BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

CONTENTS

Using this Guide 12
Documentation Set 12
Guide Conventions 13

SYSTEM OVERVIEW 14

The SmartSwitch Remote Access Module 15
The SmartSwitch Remote Access Module Network 15
9W006 and 9W007 Functionality 16
Telco Interfaces 16
Digital Modem 17
Management 17
Additional Software 18
Unique System Features 18
Interoperability Overview 20
Interoperability Protocols 20
Interoperability Devices 21
Security Overview 21
Network Interface Overview 22
System Components 23
Remote ISDN Devices 23
Switches Supported 24

Hardware Overview 25
SmartSwitch Remote Access Module Hardware 25
Available Hardware Configurations 25
Module Specifications 28
Module Interfaces 28
Module LEDs 28
SMB LED 29
Power LED 29
Ethernet 1 & 2 Activity LEDs 29
Module Ports and Connectors 30
SmartSwitch 9000 Chassis Support 30
System Management Bus (SMB-1) 31

Software Overview 32
Overview 32
System software 32
System Files 32
Configuration Files 32
Operational Files 33

Configuration Overview 35
Overview 35
SFVRA Configuration Manager 36
Starting the SFVRA-CFG Application 36
CFGEDIT 37
Executing CFGEDIT 37
Saving CFGEDIT Changes 37
Dynamic Management 38
Executing Dynamic Management 38
Utility Dynamic Management Commands 38
Saving Dynamic Management Changes 39

SYSTEM INSTALLATION 40

Ordering PRI ISDN Service (US Only) 41

Hardware Installation 43
Overview 43
Installing the SmartSwitch Remote Access Module 43
Unpacking the SmartSwitch Remote Access Module 43
Installation 44
Connecting the Module's Cabling 44
Module to SmartSwitch 9000 Ethernet Cabling 45
Mod-Tap Adapter 45
Module to PRI Service Cabling 45
Restarting the SmartSwitch Remote Access Module 46

Accessing the SmartSwitch Remote Access Module 47
Overview 47
Accessing a New Module 47
Initial Assess Using a PC and a Terminal Application 47
Initial Access Using Telnet 47
Establishing an Administration Session 48
Assigning the Module's IP Address 48
Accessing the Release Notes 49
Remote Access using Telnet 49

Upgrading System Software 50
Overview 50
Telnet Connection 50
Upgrading Software 50
Accessing the Release Notes 51

TROUBLESHOOTING 52

System Verification 53
Overview 53
Verifying Hardware Resources are Operational 53
Verifying WAN Lines are Available for Use 54

Verifying LAN Connection is Operational 55
Verifying Bridge is Initialized 55
Verifying IP Router is Initialized 56
Verifying a Dedicated Connection 56
Verifying Remote Device Connectivity 57
Verifying IP Routing Over Interfaces 57
Verifying IP Routing Over a LAN Interface 57
Verifying IP Routing Over a WAN Interface 58
Verifying IP Routing Over a WAN Remote LAN Interface 60
Verifying IP Routing Over a WAN UnNumbered Interface 61
Verifying IP RIP 62
Verifying IP RIP is Initialized 62
Verifying IP RIP Output Processing on a LAN Interface 62
Verifying IP RIP Input Processing on a LAN Interface 64
Verifying IP RIP Output Processing on a WAN Interface 65
Verify IP RIP Input Processing Operational on a WAN Interface 66
Verifying IPX Router is Initialized 66
Verifying IPX Routing is Operational 67
Verifying IPX Routing over a LAN Connection 67
Verifying an IPX Remote LAN Connection 68
Verifying IPX Routing over a WAN Connection 68
Verifying Triggered RIP/SAP 69
Verifying the AppleTalk Routing Feature 69
Verifying AppleTalk Routing is Initialized 69
Verifying AppleTalk Routing is Operational 70
Verifying AppleTalk Routing Operational over the LAN connection 71
Verifying AppleTalk Routing Operation over a WAN connection 71
Verifying SNMP is Operational 72
Verifying the Dial Out Feature 73
Verifying Compression is Operational 73
Verifying Reserved Bandwidth is Operational 73
Verifying a Semipermanent Connection 74

Problem Diagnosis 75
Overview 75
WAN Adapter 75
LAN Adapter 75
Bridge Initialization 76
IP Routing Initialization 76
WAN Line Availability 78
Dedicated Connections 80
Remote Device Connectivity 80
LAN Attachment 82
IP Routing Over Interface Connections 82
IP Routing Over the LAN Interface Connection 82
IP Routing Over a WAN Interface Connection 84
IP Routing Over a WAN RLAN Interface Connection 86
IP Routing Over a WAN UnNumbered Interface Connection 87

IP RIP 88
IP RIP Initialization 88
IP RIP Output Processing on a LAN Interface 88
IP RIP Input Processing on a LAN Interface 90
IP RIP Output Processing on a WAN Interface 90
IP RIP Input Processing on a WAN Interface 91
IPX Routing 91
IPX Routing Initialization 91
IPX Routing over the LAN Connection 92
IPX Routing over the Remote LAN Connection 93
IPX Routing over the WAN Connection 95
Triggered RIP / SAP Start Up 95
Triggered RIP / SAP Operation 95
AppleTalk Routing 96
AppleTalk Routing Initialization 96
AppleTalk Routing Operational over the LAN connection 97
AppleTalk Routing Operational over the WAN connection 100
SNMP 101
Dial Out 105
Compression 107

System Messages 109
Overview 109
Informational Messages 109
Initialization Messages 110
Normal Operation Messages 110
Spanning Tree Messages 110
Warning Messages 110
Error Messages 110
System Message Summary 110

Trace Messages 168
Overview 168
Call Trace Messages 168
Call Trace Message Summary 169
PPP Packet Trace Messages 175

SYSTEM MAINTENANCE 178

Remote Management 179
Overview 179
SNMP 180
Installation and Configuration 180
Usage Instructions 181
Telnet 182
Installation and Configuration 183
Usage Instructions 183
WIN95 Dial-Up Networking 185
Setting up a New Number 185
Setting Up Server Type 185
Dialing Out 185

TFTP 186
Installation and Configuration 186
Usage Instructions 187
Carbon Copy 188
Installation and Configuration 188
Changing CARBON COPY Configuration Parameters 188
CARBON COPY Configuration Parameters for Modem Usage 189
Usage Instructions 190
Establishing a Remote Administration Session 190
Terminating a Remote Administration Session 191
Performing a File Transfer Using CARBON COPY 192
Running without Carbon Copy 193
Removing Carbon Copy 193
Null Modem Connection 193
Adding Carbon Copy 194

System Commands 195
Overview 195
Accessing Administration Services 195
Setting the IP Address 196
Viewing Operational Information 196
Viewing Throughput Information 200
Throughput Monitor Contents 201
Saving Operational Information 202
Clearing Operational Information 202
Terminating and Restarting the SmartSwitch Remote Access Module 203
Setting the Date and Time 203
Terminating Administration Sessions 204
AppleTalk Routing Commands 205
Bridge Commands 209
Call Control Commands 210
Call Restriction Commands 213
Compression Information Commands 214
Digital Modem Commands 214
IP Routing Commands 215
IPX Routing Commands 219
ISDN Usage Commands 221
LAN Commands 222
Packet Capture Commands 222
SNMP Commands 225
Spanning Tree Commands 225
Spanning Tree Port Information 226
Spanning Tree Bridge Information 226
TCP Commands 228
Telnet Commands 228
Terminal Commands 231
TFTP Commands 232
Trace Commands 233
UDP Commands 234
WAN Commands 234

System Statistics 236
Overview 236
Connectivity Statistics 236
Call Restriction Statistics 237
Call Statistics 237
Throughput Monitoring Statistics 237
AppleTalk Statistics 238
AppleTalk Protocol Statistics 238
AppleTalk Data Delivery Protocol (DDP) Statistics 238
AppleTalk Echo Protocol (AEP) Statistics 239
AppleTalk Routing Table Maintenance Protocol (RTMP) Statistics 240
AppleTalk Zone Information Protocol (ZIP) Statistics 240
AppleTalk Name Binding Protocol (NBP) Statistics 241
AppleTalk Transaction Protocol (ATP) Statistics 241
AppleTalk Port Statistics 242
Bridge Statistics 243
Compression Statistics 243
Compression Related Statistics 244
Decompression Related Statistics 244
Digital Modem Statistics 245
LAN Statistics 245
IP Statistics 245
IP Group Statistics 246
ICMP Group Statistics 247
IPX Statistics 249
IPX General Statistics 249
IPX Basic System Table Statistics 249
IPX Advanced System Table Statistics 250
IPX RIP Statistics 251
IPX Triggered RIP Statistics 251
IPX Route Statistics 252
IPX SAP Statistics 252
IPX Triggered SAP Statistics 253
IPX Service Statistics 253
RIP Statistics 254
RIP Global Statistics 254
RIP Interface Statistics 254
SNMP Statistics 255
TCP Statistics 257
TFTP Statistics 258
Statistics for Server or Remote initiated TFTP Activity 258
Statistics for Local or Client Initiated TFTP Activity 259
Statistics for all TFTP Activity 259
UDP Statistics 260
WAN L1P Statistics 260
PRI S/T (T1/E1) Interface Statistics 260
Layer 1 PRI Error Statistics 261
Layer 1 General Statistics 262
WAN Statistics 262

Routine Maintenance 264
Overview 264
Installing/Upgrading System Software 264
Configuration Backup and Restore 264
Obtaining System Custom Information 264

APPENDICES 265

Getting Assistance 266
Reporting Problems 266
Contacting Cabletron Systems 266

Administrative Console Commands Table 268

Cause Codes Table 273

INDEX 280

USING THIS GUIDE

The *User's Guide* is divided into the following parts:

SYSTEM OVERVIEW

We begin with an overview of bridging, layer 3 switching, and specific SmartSwitch Remote Access Module features. Next, we provide an overview for the system software, the system hardware, and configuration tools. Finally, we provide an overview describing the available methods for configuring your module.

SYSTEM INSTALLATION

In this section of the *User's Guide* we provide guidelines for ordering ISDN service in the US, and a step-by-step description of installing hardware and upgrading software.

TROUBLESHOOTING

Troubleshooting begins with information for verifying your system installation, and continues with steps to take if there are problems with the installation. Next, it includes a description of system messages and trace messages. Each message listing in these chapters provides the message itself, a message definition, and where appropriate, possible corrective actions.

SYSTEM MAINTENANCE

In this section, we provide information to help you maintain your SmartSwitch Remote Access Module once it is operating. System maintenance information includes information regarding remote management, a chapter on both the system commands and the system statistics, and routine maintenance procedures.

APPENDICES

The *User's Guide* provides the following appendices:

GETTING ASSISTANCE

This appendix provides information for getting assistance if you run into problems when installing your system. A FAX form is included. You can print this form, fill out the information requested, and FAX it to Cabletron Systems, using the provided FAX number.

ADMINISTRATION CONSOLE COMMANDS

Provides a tabular listing of the system administration console commands and their uses.

CAUSE CODES

Provides a tabular listing of Q.931 Cause Codes and their meanings. These cause codes may appear in call trace messages.

DOCUMENTATION SET

This guide, the *User's Guide*, provides information to install and configure your system. It also provides information you may need to refer to keep your system running efficiently after it is up and running. For example, it provides a listing of system messages. Each message listing provides a definition of what the message means, and where appropriate, corrective action you can take. Many other subjects are covered, including routine maintenance, hardware information, system verification, and problem diagnosis.

This guide is one integral part of the entire documentation set. Please refer to the documents described below for additional information.

The *Quick Start* provides abbreviated installation and configuration instructions for experienced users. Specific instructions for setting up various types of remote devices are also included.

The *SFVRA Configuration Manager User's Guid*e provides detailed information for installing, configuring, and using the SFVRA Configuration Manager (SFVRA-CFG). SFVRA-CFG is a separate software product that is provides a GUI interface for configuring the SmartSwitch Remote Access Module. Through the SFVRA-CFG, the network administrator can deploy and maintain an entire network through a centrally located device. The network administrator can generate each system's configuration files separately, with the system's view of the network, then transfer the configuration files electronically to the system. This guide is included on the SmartSwitch Remote Access Module CD.

The *SFVRA Connection Manager User's Guide* provides detailed information for installing, configuring, and using the SFVRA Connection Manager (SFVRA-CONN). SFVRA-CONN is a separate software product that offers state of the art policy-based management system for large central site dial-in networks. This software provides a rich set of network configuration, management, and reporting capabilities. This guide is included on the SmartSwitch Remote Access Module CD.

The *Release Notes* provide release highlights and important information related to this release. The Release Notes may be displayed during software installation (or upgrade). They may also be displayed after the system is operating by issuing the *`list rel_note.txt`* console command.

GUIDE CONVENTIONS

The following conventions are used throughout the documentation:

System Commands
All system commands (Administration and Manage Mode commands) are italicized, and in a different font than the general text. For example, if you are instructed to enter the command to test for proper LAN connections, the command would appear as follows:

`lan stats`

MONITOR DISPLAYS
Any messages or text that is displayed on your monitor will be shown in the style below:

```
LAN Port <port #> is now in the LISTENING state
WAN Port <port #> is now in the FORWARDING state
LAN Port <port #> is now in the LEARNING state
LAN Port <port #> is now in the FORWARDING state
```

DOCUMENTATION TITLES
All references to SmartSwitch Remote Access Module documentation titles will use the same font as normal text, but will be italicized. For example, all references to the User's Guide will appear as:

User's Guide

SYSTEM OVERVIEW

We include the following chapters in the *System Overview* segment of the *User's Guide.*

- *The SmartSwitch Remote Access Module*
  Provides the "big picture" view of a SmartSwitch Remote Access Module network. We include an overview of unique system features, interoperability, security, interfaces, system components, remote devices, and switches supported.

- *Hardware Overview*
  A description of the 9W006 and 9W007 SmartSwitch Remote Access Modules.

- *Software Overview*
  A description of the SmartSwitch Remote Access Module's system and administrative software. We also include a description of system files.

- *Configuration Overview*
  A description of the different tools that can be used for configuration of the SmartSwitch Remote Access Module.

THE SMARTSWITCH REMOTE ACCESS MODULE

Because of the strong personal computer presence in the business environment, a move to graphical user interfaces, and the need to make the best use of available resources, there is a growing demand for high speed LAN access for remote devices. PC users need to be part of a work-group or enterprise LAN, and remote access from home, field offices, and other remote locations has become a necessity.

With the demand for remote LAN access, the remote device's requirement for bandwidth has exceeded the capabilities of traditional analog modems. High-speed digital dedicated lines can certainly provide sufficient bandwidth for LAN interconnection. However, because of the high monthly charges associated with dedicated services, the costs are prohibitive for individual users.

New forms of networking are now possible and affordable using the Integrated Services Digital Network (ISDN). ISDN is being deployed by major telecommunications companies world-wide. With ISDN services, the costs of LAN interconnection are based on actual usage — the user gets the bandwidth of dedicated digital service at dial-up prices.

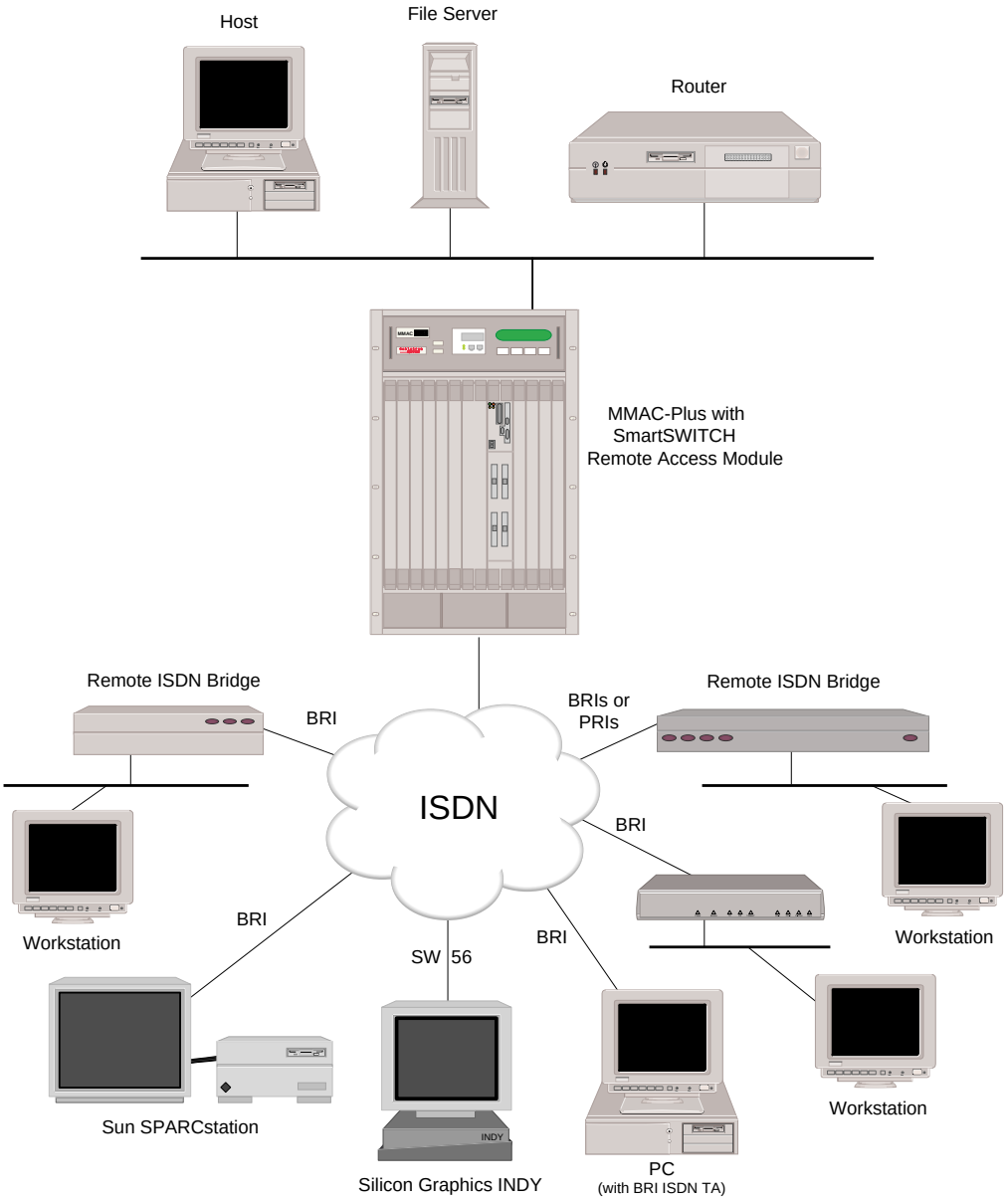
Our products offer internetworking solutions for small businesses as well as large corporations.

The SmartSwitch Remote Access Modules are versatile wide area networking products designed for the SmartSwitch 9000. They provide SmartSwitch 9000 users with an integrated solution for both LAN and WAN access. Their capabilities and performance match the requirements that high-end network connectivity users expect. The 9W006 and 9W007 expand the SmartSwitch architecture to provide ISDN and analog modem access. The analog modem access is provided via digital modem technology, and can be supported over ISDN or channelized T1 lines.

The 9W006 and 9W007 SmartSwitch Remote Access Modules are installed directly into the SmartSwitch 9000. They include four flexible WAN interfaces providing ISDN, analog modem (via digital modem), and T1/E1 or channelized T1 access. The 9W006 can support up to 96 simultaneous switched digital connections, and up to 48 simultaneous switched digital/analog modem connections. The 9W007 can support up to 120 simultaneous switched digital connections, and up to 60 simultaneous switched digital/analog modem connections.

THE SMARTSWITCH REMOTE ACCESS MODULE NETWORK

The SmartSwitch Remote Access Module can be used with a mix of bridges, routers, hosts, PCs, and workstations. These combinations provide internetworking capabilities that will allow devices to carry out LAN-to-LAN applications such as telecommuting, electronic mail, multi-media transmission, Imaging, and CAD. Devices "dial up" into a single system using a multi-line hunt group to extend the capabilities offered by an enterprise LAN.



9W006 AND 9W007 FUNCTIONALITY

TELCO INTERFACES

The telco interfaces provide the 9W006 and 9W007 SmartSwitch Remote Access Modules with an interface to telephone company-supplied ISDN PRI lines, or with unchannelized or channelized T1/E1 lines.

Depending on the country where the PRI service is offered, each PRI line supports either the 23 or 30 64Kbps B-channels for data, plus one 64Kbps D-channel for signaling.

The 9W006-220 (the 9W006 with two PRI interfaces and two digital modem interfaces) allows channelized T1 service with robbed-bit signaling for users wanting to support analog modem calls without concurrent ISDN support.

DIGITAL MODEM

The module's digital modem capability allows analog modems to be intermixed with ISDN as required to best fit specific user situations.

Up to sixty 56Kbps digital modem connections are supported. The digital modem is connected internally to the telco interface (ISDN PRI or channelized T1) eliminating the need for separate analog telco connections.

When the modules identify that a call is coming from an analog modem, the associated ISDN B-channel or channelized T1 SD0 data stream is then assigned to one of the digital modems. All of the operations of a 56Kbps modem are performed just as if the call had gone to an analog modem through an analog phone line (although at the higher speeds available with digital modem technology).

Similarly, data coming into the modules (typically from the LAN) is converted to Async-PPP, sent to the digital modem for modulation, and sent out the ISDN B-channel or T1 DS0 on the telco line.

The K56flex digital modem protocol provides automatic rate detection / negotiation such that lower baud rates are fully supported. The digital modem also supports MNP4 and V.42 error control protocols, and MNP5 and V.42bis data compression protocols.

MANAGEMENT

The SmartSwitch Remote Access Module includes *SFVRA-CFG*, a management software with flexible bandwidth management designed to keep performance up and cost down. Network managers can configure a variety of parameters to control connections being established and terminated including restrictions by packet type, time of day, and maximum calls per day.

The management capabilities included allow great flexibility. Each B channel can be used to connect to one or more single remote locations, or through inverse multiplexing higher bandwidth can be provided to users in multiples of 64Kbps.

Users can also configure the modules to sense data traffic needs and automatically initiate or terminate calls. This provides bandwidth-on-demand resulting in high performance with minimal associated cost. The management of these calls is extremely important for minimizing ISDN phone charges.

Remote management capabilities are also supported for centralized administration of decentralized networks including the use of standards such as SNMP and Telnet.

The 9W006 and 9W007 modules provide numerous network management features. Internally, Call Detail Recording will log data to a local file. Using Syslog users can capture essential data regarding remote users connection time. Also supported is Telnet with password, host and terminal server as well as tftp for the ability to upload and download log files. CDR files provide tracking and

troubleshooting capabilities while the system is up and running. The modules also support SNMP with both MIB II, private extensions, and a container MIB indicating the current configuration.

ADDITIONAL SOFTWARE

Cabletron also supplies two separate software products that are used in conjunction with the SmartSwitch Remote Access Modules: SFVRA Configuration Manager (SFVRA-CFG) and SFVRA Connection Manager (SFVRA-CONN).

SFVRA-CFG provides a GUI interface for configuring the SmartSwitch Remote Access Module. Through the SFVRA-CFG, the network administrator can deploy and maintain an entire CyberSWITCH network through a centrally located device. The network administrator can generate each system's configuration files separately, with the system's view of the network, then transfer the configuration files electronically to the system.

SFVRA-CONN offers state of the art policy-based management system for large central site dial-in networks. This software provides a rich set of network configuration, management, and reporting capabilities. The functionality of SFVRA-CONN software includes policy-based connectivity management, virtual networking that spans multiple modules (including multiple SmartSwitch 9000 chassis, and even including multiple geographic sites) with audit/accounting capabilities.

UNIQUE SYSTEM FEATURES

The SmartSwitch Remote Access Module combines unique features that improve cost-effectiveness, reliability, and performance for wide area network connections to remote devices. These features include:

- Authentication Servers
  Provide a central database for networks with more than one SmartSwitch Remote Access Module. The central database consists of manageable, informational data (referred to as the Device List or Device Table). This data is accessed and used for authentication when a new connection is established to the system.

- Bandwidth Agility
  The system dynamically controls the bandwidth in use between itself and other PPP devices. This is accomplished by establishing and disconnecting calls. The number of calls is limited only by the types and number of lines available. The system monitors the connections for utilization and will add and remove the connections based on user-configurable throughput parameters. As network bandwidth requirements increase or decrease, the system will automatically adjust the number of network connections. Thus, your network costs will reflect the actual bandwidth being used.

- Data Compression
  Allows the system to negotiate compression algorithms with another device on the network. After successfully negotiating compression, data is compressed by the remote device and transmitted to the system. The system decompresses the data, processes the information contained in the user data, and forwards the data as required. The system can receive data coming over a WAN or a LAN, and compress the data before transmitting it to another device on the network. The net effect is to increase interconnect bandwidth by decreasing transmission time. If negotiation for compression fails, data is transmitted uncompressed.

- Dial Out Capability
  The system will dial out to remote devices. This feature allows the system to accept user data received on the Ethernet LAN or ISDN network and initiate a data connection to the remote device specified in the user data. This allows devices on the local LAN to initiate connections to networks connected to the system over the switched digital network. The system monitors the connection for utilization and will remove the connection when it becomes idle.

- Digital Modem
  The system becomes an analog modem pool through its digital modem option. The system supports analog modem calls for high density channelized T1 lines using Robbed-Bit Signaling. It also supports 56Kbps digital modem technology (K56flex) with auto negotiation to automatically adapt to various modem speeds. The digital modem adapter consists of both hardware and software elements to support up to 48/60 analog and/or digital connections in each dual-slot module.

- Dynamic Management
  Provides a "real-time" management mechanism that allows many system parameters to be changed without interrupting the current execution state of the system software. This feature consists of a series of console commands that enable a user to display current system parameters, change many parameters dynamically, and write changes to disk files so that they remain permanent.

- High Speed Digital Connections
  The system supports 56Kbps and 64Kbps connections to remote locations. These dial-up digital connections provide reliable high throughput connections for efficient data transfer for the same cost as analog connections. If any remote devices connected to the system support multi-link PPP, up to 32 parallel connections can be made at either 56Kbps or 64Kbps.

- Hot Swappable Modules
  SmartSwitch Remote Access Modules are hot swappable. SFVRA Configuration Manager (VRA-CFG) can retain the configuration and setup of the module and automatically download the required information to a replacement module.

- Inverse Multiplexing
  The modules provide inverse multiplexing for both ISDN and analog modem connections supporting an aggregated bandwidth in multiples of 56/64Kbps.

- Layer 3 Switching Support
  The SmartSwitch Remote Access Modules provide layer 3 switching support for IP, IPX, and AppleTalk. Also provided is multiprotocol layer 2 switching.

- Packet Capture
  In order to monitor incoming LAN data, the SmartSwitch Remote Access Module packet capture feature will allow you to capture, display, save, and load bridged or routed data packets.

- Protocol Discrimination
  It is possible for multiple types of remote devices to use the same line. The system can determine the device type and the protocol encapsulation used by remote devices.

- Security
  Security is a key issue for all central site network managers and is a priority with the SmartSwitch Remote Access Modules. The modules provide high level features that help prevent unauthorized or inadvertent access to critical data and resources. The modules support extensive security levels including:
  - PPP PAP and CHAP
  - User name and password
  - Calling Line ID (CLID)
  - Ethernet Address
  - User Authentication
  - Device Authentication
  - SecureFast Virtual Remote Access (SFVRA)

- Simultaneous Connections
  The system supports simultaneous connections to multiple locations. These locations can connect by using different channels on the same line, or they can connect on different lines. This pooling of lines among many potential locations is more cost effective than alternative point-to-point lines.

INTEROPERABILITY OVERVIEW

"Interoperability" is the ability to operate and exchange information in a heterogeneous network. The SmartSwitch Remote Access Module supports interoperability with many different remote devices over ISDN.

INTEROPERABILITY PROTOCOLS

In order to communicate with various remote devices over ISDN, the SmartSwitch Remote Access Module must identify the device type and the protocol it is using.

The SmartSwitch Remote Access Module supports the following line protocols:
- HDLC Ethernet Frames
- Ordered Protocol for Ethernet Frames
- RFC1294 Based Encapsulation for IP Datagrams
- Point-to-Point Protocol (PPP) Encapsulation for IP Datagrams

The SmartSwitch Remote Access Module supports the following PPP protocols:
- Link Control Protocol (LCP)
- Multilink Protocol (MLP)
- Authentication Protocols
  - Challenge Handshake Authentication Protocol (CHAP)
  - Password Authentication Protocol (PAP)
- Network Control Protocols (NCP)
  - Internet Protocol Control Protocol for TCP / IP (IPCP)
  - Internetwork Packet Exchange Control Protocol for IPX (IPXCP)
  - Bridge Control Protocol for bridges (BCP)
- Compression Control Protocol (CCP)
- AppleTalk Control Protocol (ATCP)

The SmartSwitch Remote Access Module supports the following AppleTalk protocols:
- EtherTalk Link Access Protocol (ELAP)

- AppleTalk Address Resolution Protocol (AARP)
- PPP AppleTalk / AppleTalk Control Protocol (ATCP)
- Datagram Delivery Protocol (DDP)
- Routing Table Maintenance Protocol (RTMP)
- AppleTalk Echo Protocol (AEP)
- Name Binding Protocol (NBP)
- Zone Information Protocol (ZIP)

INTEROPERABILITY DEVICES

Remote devices that may connect to the SmartSwitch Remote Access Module include the following:

- MAC Layer Bridges
- IP Host Devices
- IP Router Devices
- IPX Routers
- AppleTalk Routers

MAC layer bridges connect to the system using the HDLC bridge encapsulation line protocol. These devices send transparently bridged Ethernet frames to the system. MAC layer bridges do not process network layer protocols. They forward all packets based on source and destination MAC addresses.

IP Host devices are single workstations or PCs that connect to the system at the IP network layer. These devices use either the RFC1294 based protocol or PPP to communicate with the system.

IP router devices are single devices that represent many other IP hosts and routers to the system. They must use the CHAP or PAP protocol to identify themselves to the system. IP routers usually provide IP network address information at connection time (and use PPP to send user data to the system).

IPX routers are single devices that perform network layer tasks (addressing, routing, and switching) to move packets from one location on the network to another. IPX routers use the Internetwork Packet Exchange (IPX) protocol, typical of the NetWare environment.

AppleTalk routers route AppleTalk datagrams based on address information. They support the following protocols: RTMP, NBP, and ZIP.

SECURITY OVERVIEW

The system provides several options for validating remote devices and for managing network security. The security options available are dependent on the remote device type, type of access, and the level of security required.

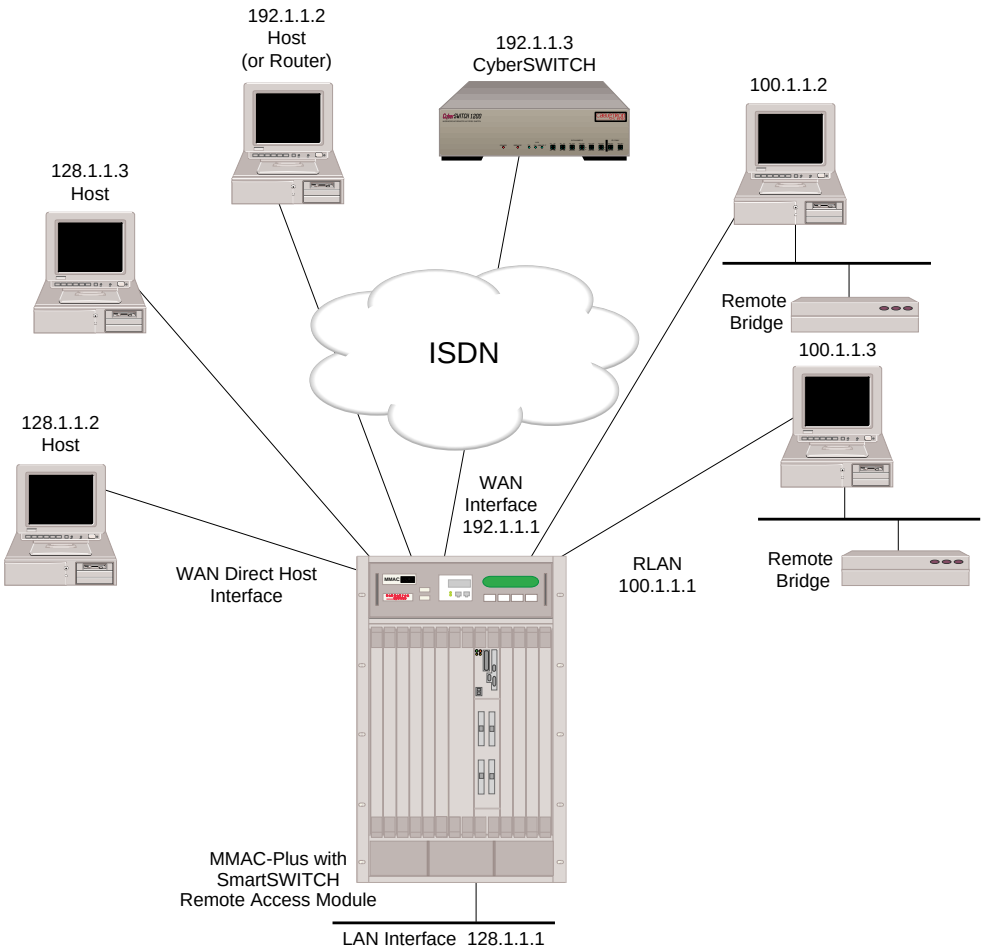
NETWORK INTERFACE OVERVIEW

The network interface is the physical connection of the SmartSwitch Remote Access Module to a data network. For example, the Ethernet resource in the system provides a network interface to an Ethernet LAN. The ISDN lines in the system provide network interfaces to multiple remote networks. Because of their switched nature, the ISDN lines provide virtual network interfaces. That is, the same physical ISDN line can actually connect to different remote networks by dialing a different phone number.

The SmartSwitch Remote Access Module provides a set of network interfaces that give you a wide range of flexibility. The network interfaces provided by the system are:

- LAN IP Network Interface
- LAN IPX Network Interface
- WAN IP Network Interface
- WAN RLAN IP Network Interface
- WAN RLAN IPX Network Interface
- WAN (UnNumbered) Network Interface

The variety of network interfaces allows the installation of a wide range of devices at remote sites. As illustrated below, you can simultaneously choose bridges, routers, or host devices based on the specific remote site requirements.



In the diagram above, the LAN Interface 128.1.1.1 is attached to the IP network 128.1.0.0. The WAN Direct Host Interface represents LAN Interface 128.1.1.1 and allows the remote IP hosts to share the network address space of 128.1.0.0. The WAN Interface 192.1.1.1 is logically attached to the IP network 192.1.1.0. The RLAN Interface 100.1.1.1 is logically attached to the IP network 100.1.1.0.

SYSTEM COMPONENTS

The major components of the SmartSwitch Remote Access Module are:

- System hardware consisting of a module and an administration port provided by the platform.
- System software specific to the SmartSwitch Remote Access Module, adapter modules, and administration functions.
- Administration software that provides configuration, diagnostics and maintenance on the system.
- System files containing configuration and operational information.
- Remote ISDN devices which interoperate with the system and allow device access to network resources.

More detailed descriptions of system software and hardware are included in the next two chapters. The following section describes remote ISDN devices.

REMOTE ISDN DEVICES

The SmartSwitch Remote Access Module provides a centralized concentrator function for remote ISDN devices. The devices can be separated into the following categories:

- remote ISDN bridge devices
- PC based terminal adapters
- ISDN enabled workstations
- other ISDN routers

Typical remote ISDN bridges provide one Ethernet port and one basic rate ISDN port. The basic rate port is connected to the switched digital network and is used to make connections to the SmartSwitch Remote Access Module. The Ethernet port is used to connect to a remote LAN. The remote bridge device sends Ethernet frames from devices on the remote LAN over the switched network.

PC-based terminal adapters connect to a remote personal computer and use the switched digital network to connect to the system. The terminal adapter sends network protocol specific frames from the host PC device over the switched network.

Workstation-based terminal adapters connect to a workstation and use the switched digital network to connect to the system. The terminal adapter sends network protocol specific frames from the workstation over the switched network.

SWITCHES SUPPORTED

The SmartSwitch Remote Access Modules support the following ISDN PRI switch types:

- AT&T Definity
- AT&T 4ESS
- AT&T 5ESS
- DMS250
- DMS100
- SL100
- NET5
- 1TR6
- NTT INS
- TSO 14

HARDWARE OVERVIEW

The SmartSwitch Remote Access Modules are versatile wide area networking products designed for the SmartSwitch 9000. They are installed directly into the SmartSwitch 9000, expanding the SmartSwitch 9000 architecture to provide ISDN and analog modem access.

This chapter provides a description of the following:

- module hardware
- SmartSwitch 9000 chassis support for the modules
- System Management Bus (SMB)

For installation instructions, refer to *Hardware Installation*.

SMARTSWITCH REMOTE ACCESS MODULE HARDWARE

This section provides an overview of the module's hardware by describing the SmartSwitch Remote Access Module's:

- available hardware configurations
- hardware characteristics
- interfaces
- LEDs
- ports and connectors

AVAILABLE HARDWARE CONFIGURATIONS

There are two families of SmartSwitch Remote Access Modules: the 9W006 modules for countries using T1 lines, and the 9W007 modules for countries using E1 lines. Each module family consists of three possible configurations for remote access connectivity. We summarize the possible configurations for each module family below.

The 9W006 module configured for T1 countries and is available in the following configurations:

- 9W006-200
  This model provides an interface for two ISDN PRI or T1 lines (either unchannelized or channelized) supporting up to 46 or 48 connections.

- 9W006-400
  This model provides an interface for four ISDN PRI or T1 lines (either unchannelized or channelized) supporting up to 92 or 96 connections.

- 9W006-220
  This model provides an interface for two PRI or T1 lines (channelized), and two digital modems (24-port) supporting up to 46 or 48 digital or analog connections.

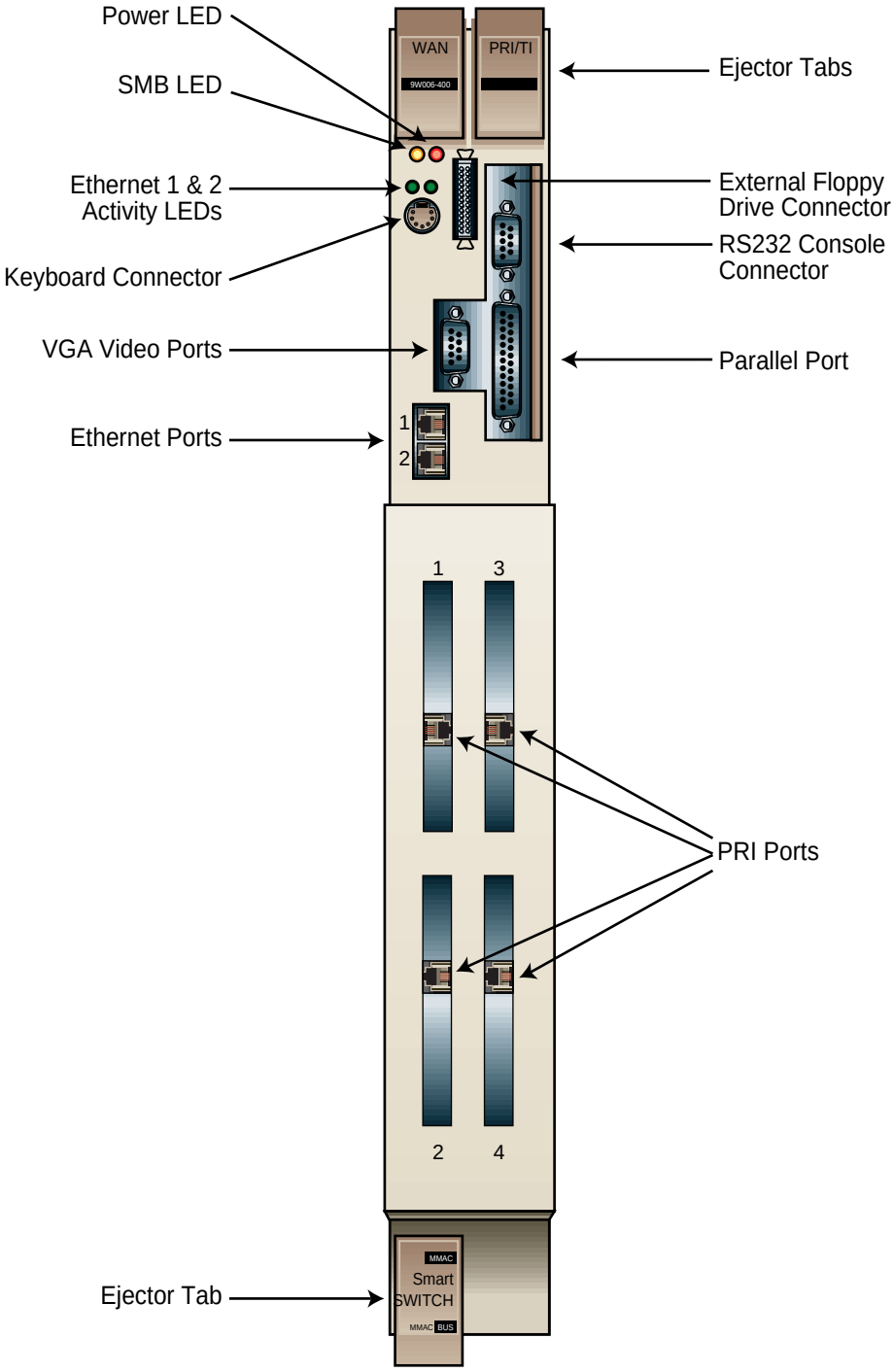
The 9W007 module is configured for E1 countries and is available in the following configurations:

- 9W007-200
  This model provides an interface for two ISDN PRI or E1 lines (either unchannelized or channelized) supporting up to 60 connections.

- 9W007-400
  This model provides an interface for four ISDN PRI or E1 lines (either unchannelized or channelized) supporting up to 120 connections.

- 9W007-220
  This model provides an interface for two PRI or E1 (channelized), and two digital modems (30-port) supporting up to 60 digital or analog connections.

The following graphic illustrates the 9W006-400 module. Note that the 9W007-400 has identical physical features (connectors, ports, etc.). The remaining modules have the same physical features with the exception of the configuration of the WAN interface ports. The 9W006-200 and the 9W007-200 have two PRI interfaces, as does the 9W006-220 and 9W007-220 (their modem interfaces are internal).



The 9W006-400

MODULE SPECIFICATIONS

Physical Characteristics

Height:	45.72 cm (18 in)
Width:	13.97 cm (5.5 in)
Depth:	44.45 cm (17.5 in)
Weight:	10.35 kg maximum (23 lb.)

Environmental Characteristics

Operating Temp:	5° to 40° C (41° to 104° F)
Operating Humidity:	20 to 95% non-condensing

Regulatory Compliance

Meets or exceeds the following:

Safety:	UL 1950, CSA C22.2 No. 950, EN 60950, IEC 950, and 72/23/EEC
EMI:	FCC Part 15, EN 55022, CSA 108.8, EN 50082-1, VCCI V-3, and 89/336/EEC

MODULE INTERFACES

The SmartSwitch Remote Access Module includes the possibility of four flexible WAN interfaces providing ISDN, analog modem (via digital modem), and T1/E1 or channelized T1 access. As described earlier, depending on the model, the module may have one of the following interface configurations:

- four PRI interfaces
- two PRI interfaces
- two PRI interfaces and two digital modems

PRI interfaces provide the module with an interface to telephone company-supplied ISDN Primary Rate Interface (PRI) lines, or with unchannelized or channelized T1/E1 lines. Each PRI interface supports up to 23 B channels for data and a 64Kbps signaling D channel (for countries using T1 lines), or up to 30 B channels for data and a 64 Kbps signaling D channel (for countries using E1 lines). The module uses the B channels for switched connections to carry device data. PRI interfaces have an external port for connecting to the Telco interface.

Digital modem interfaces allow the SmartSwitch Remote Access Module to receive calls from asynchronous PPP remote devices connected by modem. Each digital modem interface supports up to 24 56Kbps modem connections (for countries using T1 lines), or up to 30 56Kbps modem connections (for countries using E1 lines). Digital modem interfaces are connected internally to the PRI interface eliminating the need for separate analog telco connections.

MODULE LEDS

The 9W006 and 9W007 has LEDs for the following functions: SMB, power, and Ethernet activity. Refer to the illustration of the 9W0006-400 for LED locations. We describe these LEDs in the following sections.

SMB LED

The SMB LED is an indicator for the System Management Buses (SMB-1). This is a 1Mbps management bus located within the SmartSwitch 9000. It is utilized by all diagnostic controllers in the system. These include connectivity modules, power supply modules, and the environmental module. The SMB-1 transports inter-chassis information between system components, such as power and environmental information, as well as diagnostic messages. Periodic loop-back tests are performed by all modules that share this bus (which includes the SmartSwitch Remote Access Modules) to ensure the validity of SMB-1.

The functions of the SMB LED are listed in the following table.

LED Color	*Description*
green	fully operational
red	normal power-up reset
off	module powered off

POWER LED

The power LED provides information regarding the module power status. The functions of the power LED are listed in the following table.

LED Color	*Description*
green	powered on
off	module powered off

ETHERNET 1 & 2 ACTIVITY LEDS

The Ethernet 1 and 2 LEDs illuminate when the integrated Ethernet controller has activity on either the transmitting or receiving lines for that channel.

The functions of the Ethernet 1 and 2 LEDs are listed in the following table.

LED Color	*State*
green	activity on the indicated Ethernet line (1 or 2)
off	no activity on the indicated Ethernet line (1 or 2)

MODULE PORTS AND CONNECTORS

The SmartSwitch Remote Access Module's front panel has the following ports and connectors (refer to the illustration of the 9W0006-400 for locations):

- *RS232 console connector*
  You may use this connector to attach a lap top computer to the module. The lap top can then provide you with an administration console. The administration console is simply a communication path between you and the module; you can use this console to help you manage the module. For example, through the console you may enter system commands such as `dr` to display the current report log messages (a valuable diagnostic tool), or `br stats` (or one of the other statistics commands) to display system statistics.

- *external floppy drive connector*
  Software upgrades are possible through an external floppy drive connected to the module via this connector. The Cabletron external IDE drive (#EAP-EXT3.5-FD) is compatible with this connector.

- *keyboard connector, VGA video port*
  Using these connectors, you can attach a keyboard and a VGA monitor to provide a local administration console.

- *parallel port*
  This port is currently disabled.

- *dual ethernet ports*
  Using these connectors and the provided Ethernet cables, you can connect the module to the SmartSwitch 9000's Ethernet connection, giving the module presence on the LAN.

- *PRI ports*
  Used for WAN (telco) connection access to support ISDN PRI, T1/E1, and digital modem service (the digital modem interfaces connect internally to the PRI interfaces; there are no external ports for the digital modems).

SMARTSWITCH 9000 CHASSIS SUPPORT

The SmartSwitch 9000 chassis provides redundancy for a high availability system design. The 9W006 and 9W007 SmartSwitch Remote Access Modules are hot swappable. The SFVRA Configuration Manager can retain the configuration and setup of the module and automatically download required information to a replacement module. The module identity "9W000 Remote Access Module" is conveyed to the SmartSwitch 9000 management module along with serial number, MAC addresses and other identifying information.

The 9W006 and 9W007 modules connect to the SmartSwitch 9000 System Management Bus (SMB-1) and SmartSwitch 9000 Power Bus. They additionally include their own processor, 32 MB DRAM memory, and allow local management capability in addition to remote management. Software upgrades will be supported through a Telnet or remote console connection.

SYSTEM MANAGEMENT BUS (SMB-1)

The 9W006 and 9W007 SmartSwitch Remote Access Modules share information through the SmartSwitch 9000 SMB backplane permitting connectivity to the SmartSwitch 9000 Environmental Management Module to control temperature of the board, fans, humidity, and various other environmental components. The SMB-1 connection also provides visibility in Spectrum for its Module I.D., 9W000 Remote Access Module, indicating a dual-slot module. Modules can be reset or powered on or off via Spectrum allowing maintenance on a selected WAN module while the others in the SmartSwitch 9000 remain operational.

SOFTWARE OVERVIEW

OVERVIEW

The SmartSwitch Remote Access Module software provides:

- system software for the SmartSwitch Remote Access Module, LAN and WAN interfaces, and administration functions
- system files containing configuration and operational information

This chapter provides an overview for each of the above software categories.

SYSTEM SOFTWARE

Included with each SmartSwitch Remote Access Module is a CD containing upgrade software and utility software. (Note that initial system software is factory-installed). The following system software files are available on the CD:

`upgrade.osw`
All the system files needed for upgrading the SmartSwitch Remote Access Module are combined in this file.

`defltcfg.osw`
All of the system files needed to return your system configuration to the factory default are combined in this file.

SYSTEM FILES

The system files consist of the required configuration files, as well as the operational files that the SmartSwitch Remote Access Module maintains. All of these files may be accessed by using available administrative commands. (Refer to the *System Commands* chapter for details.)

Below is a brief description of the configuration and operational files.

CONFIGURATION FILES

The configuration files store the configuration data. These files are located in the system's `\config` directory. You can maintain these files by using VRA-CFG, which is delivered with the system.

The configuration files associated with the system are:

`network.nei`
This configuration file contains information about the switched network.

`devdb.nei`
This file contains the On-node Device Database configuration information about each remote device.

`node.nei`
This configuration file contains node-specific information like resources, lines, SmartSwitch Remote Access Module operating mode and security options, along with the Throughput Monitor Configuration information. If enabled, SNMP configuration information is also in this file.

`lan.nei`
This file contains configuration information used when the bridge is enabled. This file also contains information for the Spanning Tree protocol used for the bridge. Information from this file is configured and used only when the bridge is enabled.

`ip.nei`
This file contains configuration information used when the IP routing is enabled. This file also contains information regarding network interfaces, RIP, and static routes. Information from this file is configured and used only when the IP routing is enabled.

`ipx.nei`
This file contains configuration information used when the IPX routing is enabled. This file also contains information regarding network interfaces, RIP, and static routes. Information from this file is configured and used only when the IPX routing is enabled.

`filter.nei`
This file contains all filter configuration information (bridge, hardware, and IP). This file is new to Release 7.2 software, but is compatible with previous software versions, which contained filter information in the `lan.nei` and/or `ip.nei` files. With Release 7.2 configuration changes and configuration file updates, this filter information will be moved to `filter.nei`.

`atalk.nei`
This file contains configuration information used when AppleTalk Routing is enabled. This file also contains information regarding ports and static routes. Information from this file is configured and used only when the AppleTalk routing is enabled.

`sdconf.rec`
This is not a system file; it is a configuration file delivered on the ACE Server. However, you may TFTP this file to the system's `\config` directory as an alternate method of providing the system with ACE Server configuration information.

OPERATIONAL FILES

While the SmartSwitch Remote Access Module is running, it collects system statistics and logs system messages. The system maintains these statistics and messages in two separate memory-resident tables. The ten most recent versions of each table are available on the system disk.

You can retrieve and view the current memory-resident tables at any time by using the following console commands:

dr	This command will display system messages.
ds	This command will display system statistics.

You can write the tables to disk by using the following commands:

wr	This command will write the current system messages to disk.
ws	This command will write the current system statistics to disk.

Notes: You need an active administration session to issue these commands. Refer to *Accessing the SmartSwitch Remote Access Module* for instructions regarding establishing an administration session.

When the system is shut down, the tables are automatically written to disk.

The system stores the tables in ASCII format files on the System disk. When the system writes system messages to disk, it stores them in the following location:

Directory: `\log`
File Name: `rprt_log.nn`
Where "nn" is an integer that is incremented each time a new file is written.

When the system writes system statistics to disk, it stores them in the following locations:

Directory: `\log`
File Name: `stat_log.nn`
Where "nn" is an integer that is incremented each time a new file is written.

CONFIGURATION OVERVIEW

OVERVIEW

We provide the following configuration tools to set up and / or alter your configuration:

- SFVRA Configuration Manager, the graphical interface utility for basic to intermediate configurations
- CFGEDIT, the configuration utility for more complex configurations
- Manage Mode, the dynamic management utility

SFVRA Configuration Manager (SFVRA-CFG) is a fast and easy way to configure basic features for your system. However, SFVRA-CFG is NOT dynamic. This means that after the configuration files are transferred, SFVRA-CFG interrupts normal system operation in order to implement the files. It is also important to note that downloading these configuration files does not update the system's existing configuration files, it overwrites them.

The following is a list of some of the major features that cannot be configured by SFVRA-CFG:

- AppleTalk Remote LAN port
- Bridge filters
- DHCP
- File attributes configuration
- Frame Relay
- IP filters
- IPX static routes and services
- Off-node authentication databases
- TFTP configuration
- X.25

For a more complex configuration, CFGEDIT is a comprehensive utility you may wish to use to configure advanced features for your system. CFGEDIT is also NOT dynamic. This means you will have to interrupt normal system operations in order to update configuration files. (You may do so by either rebooting, or issuing the `restart` command).

WARNING:

If you use CFGEDIT to make configuration changes you will no longer be able to use SFVRA-CFG.

Manage Mode provides a real-time management mechanism that allows you to change the configuration, without interrupting the current execution state of the system software. But, because it is dynamic, Manage Mode does have its limitations. So, when making configuration changes, you usually need to use a combination of both Manage Mode and CFGEDIT.

WARNING:

If you use Manage Mode to make configuration changes you will no longer be able to use SFVRA-CFG.

You may only have one CFGEDIT or Dynamic Management session active at a time per system. For example, if a user is making changes directly to the system using Dynamic Management, and then a second person at a different location using Telnet attempts changes, access will be denied to the second person. However, if you have an active CFGEDIT or Dynamic Management session and

you use SFVRA-CFG to download configuration files, the files will be over written and the system will reboot. The CFGEDIT or Dynamic Management session will be canceled, and any changes, unsaved or saved, will be lost.

With two exceptions, it is possible to completely configure your system using CFGEDIT. The exceptions are:
1. TFTP configuration
2. file attributes configuration

These two elements can only be configured using Manage Mode.

SFVRA CONFIGURATION MANAGER

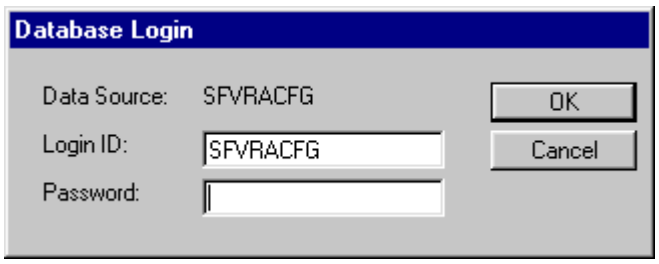
The SFVRA Configuration Manager allows a network to be configured and managed centrally. It is made up of two components: the SFVRA-CFG database (using either MS SQL Server, or MS Access) and the SFVRA-CFG client application, which is the interface to the database.

The network administrator can generate each system's configuration files separately, with the system's view of the network, then transfer the configuration files electronically to the system. SFVRA-CFG provides a mechanism to define a system at a site, based on administrator-defined templates and standard configurations. It also allows the definition of major protocol networks and their ISDN lines, mapping them to specific sites and then to systems at that site. The configuration files generated by SFVRA-CFG for a specific system can be transferred to that system using a proprietary, secure protocol. For more information on SFVRA-CFG, including installation and configuration instructions, refer to *SFVRA Configuration Manager User's Guide.*

STARTING THE SFVRA-CFG APPLICATION

To start the SFVRA-CFG:

1. Open the SFVRA-CFG application.
3. From the menu bar, click on *File* then click on *Connect*, or click on the toolbar.
4. A dialog box similar to the following will be displayed:



Note that the first time you use the SFVRA-CFG application, the login ID is set to SFVRACFG. If desired, you may edit this field to change the login ID.

5. If required, enter your password.
6. Click *OK*.

CFGEDIT

CFGEDIT is a menu-driven utility. It consists of multiple, detailed submenus which allow you to set up or change configuration parameters. To better understand the structure of CFGEDIT, refer to the *CFGEDIT Map* in the Appendix of the *User's Guide* for the Central Site CyberSWITCH.

CFGEDIT allows you to configure your system while the system software is still executing. These configuration changes are saved in a temporary copy of configuration data. At a convenient time, you may then reboot the system to make these changes permanent.

Configuration changes made using CFGEDIT are not recognized by SFVRA-CFG. Therefore, once you use CFGEDIT, you must always use CFGEDIT. This documentation is written under the assumption that you will use SFVRA-CFG. However, if you plan on using CFGEDIT, refer to the Central Site documentation, which is included on the CD-ROM for just such a purpose. In particular, note that the *System Verification* and *Problem Diagnosis* chapters of the Central Site CyberSWITCH documentation are written using CFGEDIT techniques. Also, there are three sections of configuration chapters (Basic, Security, and Advanced Configuration sections) included in the CyberSWITCH Central Site documentation that are written for the CFGEDIT configuration utility.

EXECUTING CFGEDIT

After the system software has been loaded, you can start CFGEDIT by entering the following command at the system prompt as shown below:

```
[product name]> cfgedit
```

As long as there is no other "change" session active (CFGEDIT or Manage Mode), access is granted, and the following menu is displayed:

```
 Main Menu:

   1) Physical Resources
   2) Options
   3) Security
   4) Save Changes

Select function from above or <RET> to exit:
```

From this screen you will begin the configuration process. Refer to *Basic Configuration* and succeeding chapters of the *User's Guide* for the Central Site CyberSWITCH for details on using this utility to perform specific configuration tasks.

Remember, changes to CFGEDIT are NOT dynamic. Changes are saved in a temporary copy of configuration data, and will not affect the current operation of the system in any way.

SAVING CFGEDIT CHANGES

To terminate the session, return to the main CFGEDIT menu. If you have made changes, select option 4 (*Save Changes)* before exiting. If you attempt to exit without saving, you will be prompted to do one of the following:

- save changes (Y) and exit
- do not save changes (N) and exit
- do not save changes as yet, but return to the Main Menu for further configuration <RET>

To save changes at this point, answer Y for yes:

```
Save changes and exit (Y or N)? or press <RET> for previous menu:
```

The save process also includes all unsaved Manage Mode changes which were made prior to the CFGEDIT session, if any.

At your earliest possible convenience, restart the SmartSwitch Remote Access Module. This will then activate the new configuration data.

DYNAMIC MANAGEMENT

EXECUTING DYNAMIC MANAGEMENT

The Dynamic Management feature provides a real-time management mechanism; allowing you to change the system's configuration without interrupting the execution of the system software. This feature consists of console commands that enable you to display current system parameter, change many parameters dynamically, and write changes to disk files so that they remain permanent. However, Manage Mode does have its limitations. Therefore, you will generally need to use both CFGEDIT and Manage Mode in order to make all appropriate configuration changes.

Configuration changes made using Manage Mode are not recognized by SFVRA-CFG. Therefore, once you use Manage Mode, you cannot use SFVRA-CFG. This documentation is written under the assumption that you will use SFVRA-CFG. However, if you plan on using Manage Mode, refer to the Central Site documentation, which is included on the CD-ROM for just such a purpose.

Before using Dynamic Management commands, you must first enter the special Manage Mode by typing the following command at the system prompt:

>manage

Once Manage Mode is entered, the prompt changes from `[system name]>` to `[system name]: MANAGE>`. While operating in Manage Mode, only Dynamic Management commands are available. All other system commands are ignored until you exit Manage Mode.

The `<CTRL><C>` key sequence will terminate the current command and return you to the `MANAGE>` prompt. This is useful if you are in the process of responding to a series of prompts and you wish to abort the command without responding to the remaining prompts.

Note: To use a command, you may enter the full command name as it appears in the HELP list, or you may shorten the command to the point that it can still be distinguished from all other Dynamic Management commands.

UTILITY DYNAMIC MANAGEMENT COMMANDS

There are several Manage Mode commands that are used for functions other than to configure the system. They are as follows:

cls
Clears the display screen. This command is also available as an administration command.

help
The Manage Mode help command lists the available Dynamic Management commands and instructs the user to enter the command followed by a question mark to see help information for that specific command.

readme
Displays helpful tips on how to use the Dynamic Management commands.

SAVING DYNAMIC MANAGEMENT CHANGES

The Dynamic Management commands allow system data to be changed in real-time. These changes take effect immediately upon the execution of the command and remain in effect until the system is restarted. Once a software restart occurs, the changes are lost because the software reads its initial system data values from a series of configuration files.

To prevent desired data changes from being overwritten by the restart process, the *commit* command should be executed. This command writes the current system data to the appropriate disk files, thus making all changes permanent, even if the system software is restarted.

The *commit status* command displays the number of dynamic changes that have been made using each Dynamic Management command since the last *commit* was performed.

To return to the normal operating mode after you have committed your changes, issue the following command:

```
MANAGE> exit
```

SYSTEM INSTALLATION

We include the following chapters in this segment of the *User's Guide*:

- *Ordering ISDN Service*
  Provides guidelines for ordering ISDN service in the United States.

- *Hardware Installation*
  Step-by-step instructions for installing hardware components.

- *Accessing the SmartSwitch Remote Access Module*
  Provides a description of the possible ways to access the SmartSwitch Remote Access Module (for diagnostic purposes, or for software upgrade).

- *Upgrading System Software*
  A description of the software upgrade process.

ORDERING PRI ISDN SERVICE (US ONLY)

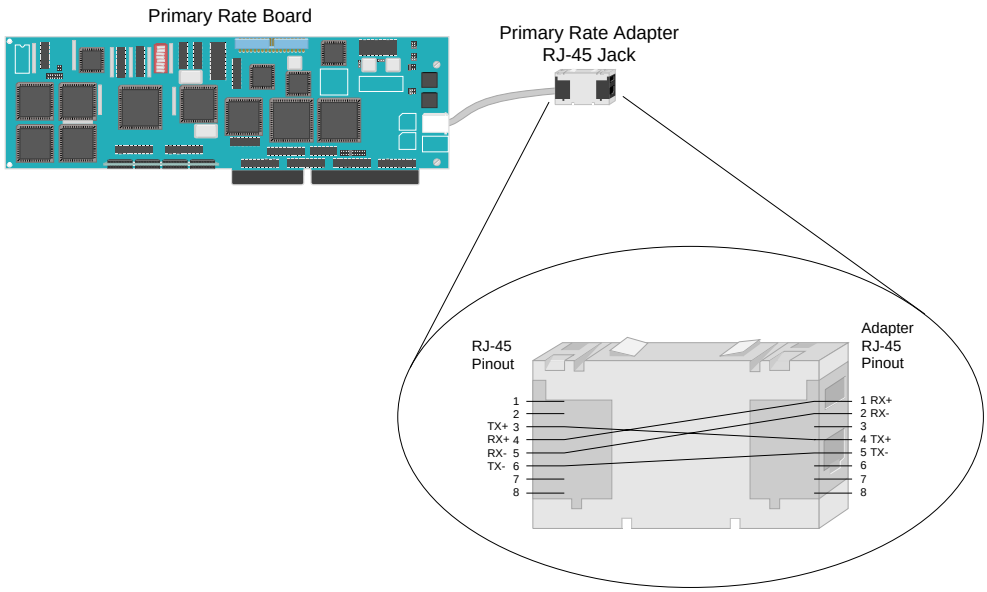
ISDN Primary Rate is a communications service that allows the system to make up to 23 connections over a single line. It uses a 4-wire T1 line that carries 24 channels, each providing 64000 bps bandwidth. The service uses channels 1 to 23 as bearer (B) channels to carry connections between two systems. The 24th channel is used for signaling information (the data link).

You should request the following options for a primary rate line that is connected directly to a SmartSwitch Remote Access Module:

- B8ZS encoding
- ESF framing
- all channels should be Circuit Switched Data
- Hunt Group (if desired)
- call bandwidth supported (56Kbps, 64Kbps, and / or 384Kbps)
- CLID (calling line Id); usually there is no charge for this

In order to connect to the primary rate line, the customer needs a Channel Service Unit (CSU), which is integrated into the SmartSwitch Remote Access Module. If the line is provided by a LEC or IXC, the CSU is required by the phone company to protect the phone network from any problems with customer premise equipment. At the time that the line is ordered, the customer may be asked for the FCC registration number for the SmartSwitch Remote Access Module that is being used.

The cabling between the wall jack and the SmartSwitch Remote Access Module is very important, and is also where most problems occur. The system's PRI RJ-45 adapter uses the international standard of pins 3, 4, 5, and 6 for transmit and receive. Most T1 lines in the United States and Europe use the traditional 1, 2, 4, and 5 pins. We provide an RJ-45 to RJ-45 Mod-Tap adapter that will convert between the two wiring systems.



For non-U.S. and European installations, a standard 4 or 8 wire cable with RJ-45 jacks is sufficient.

When the line is installed, you must ask the phone company the following questions:

1. What are the phone numbers for the line? (There may be more than one.)
2. Do I need to use any prefix when I dial? (For example, "9" for a Centrex line.)
3. What type of switch is the line connected to?
4. For #4ESS, what release of software is running on the switch?

When the phone company installs the line, they assign it certain characteristics (sometimes called translations). These are different depending on the type of ISDN switch to which the line is attached. The customer must know what type of switch is being used.

The following table provides correct settings for important configuration options.

Option	*Local Bell Operating Company*		*AT&T Network*	*U.S. Sprint & MCI*
Type of Switch	#5ESS	DMS100	#4ESS	DMS250
Encoding	B8ZS	B8ZS	B8ZS	B8ZS
Framing	ESF	ESF	ESF	ESF
Network Facilities	NA	NA	SDS or Call-By-Call	NA
Echo Cancellation	NA	NA	NA	OFF (Disabled)

HARDWARE INSTALLATION

OVERVIEW

This chapter provides a brief description of the SmartSwitch Remote Access Module hardware installation process including instructions for:

- installing the 9W006/9W007 module in to a SmartSwitch 9000
- connecting the module's cabling

In case you need to restart the module during installation, instructions are also included for restarting the module.

INSTALLING THE SMARTSWITCH REMOTE ACCESS MODULE

This section contains instructions for unpacking the SmartSwitch Remote Access Module, then guides you through installing the module into an SmartSwitch 9000. Instructions are also provided for resetting the module.

Only qualified personnel should install the SmartSwitch Remote Access Module.

The SmartSwitch Remote Access Module and the host SmartSwitch 9000 are sensitive to static discharges. Use a grounding strap and observe all static precautions during this procedure. Failure to do so could result in damage to the SmartSwitch 9000 or the module.

UNPACKING THE SMARTSWITCH REMOTE ACCESS MODULE

Unpack the SmartSwitch Remote Access Module as follows:

1. Remove the shipping box material covering the SmartSwitch Remote Access Module.

2. Carefully remove the module from the shipping box. Leave the module in its non-conductive bag until you are ready to install.

3. Attach the disposable grounding strap to your wrist and to a proper ground (refer to the instructions outlined on the grounding strap package).

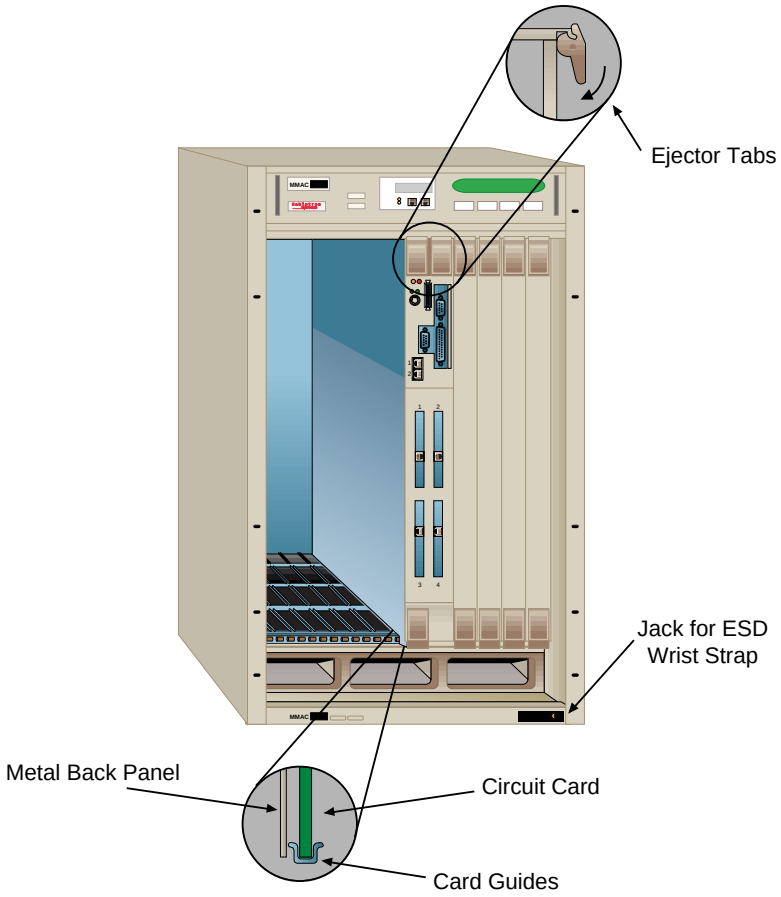
4. After removing the module from its non-conductive bag, visually inspect the device. If you notice any signs of damage, DO NOT install the module. Contact Cabletron Systems Technical Support immediately.

INSTALLATION

1. Note that the module is a double wide module and will fill two SmartSwitch 9000 slots. Remove the SmartSwitch 9000's back panels that are covering the two slots into which the module will be installed. To ensure proper airflow and cooling, all other empty slots must be covered.

2. Before installing the SmartSwitch Remote Access Module into the chassis, ensure that the bottom and top plastic tabs are unlocked.

3. Slide the module into the available slots making sure that the module is between the guides as shown in the following illustration. Check both the upper and lower tracks. Take care that the module slides in straight and engages the backplane connectors properly.



4. Lock down the top and bottom plastic tabs *at the same time, applying even pressure.*

CONNECTING THE MODULE'S CABLING

Installing the module into the SmartSwitch 9000 automatically completes its power supply and SMB connections. As you slide the module into place, the module's power supply and SMB connectors slide into the SmartSwitch 9000's power supply and its SMB-1 BUS. What you will need

to complete, though, is the Ethernet and PRI cabling. In addition, U.S. and European installations need a Mod-Tap adapter for each PRI port. Instructions for each are included below.

MODULE TO SMARTSWITCH 9000 ETHERNET CABLING

We supply two Ethernet cables with the module. You will use these cables to connect the module's Ethernet interface(s) to the SmartSwitch 9000's Ethernet connection, providing the module with LAN connectivity. To complete the Ethernet cabling:

1. Refer to the illustration of the 9W0006-400 for the Ethernet ports' locations.

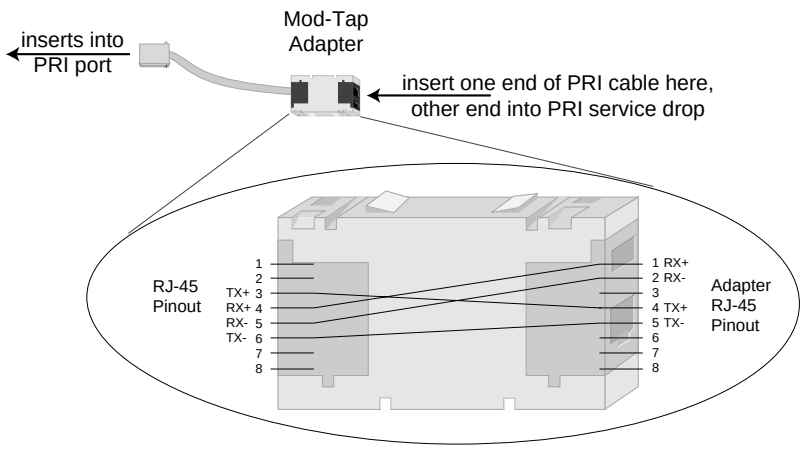
2. Insert the RJ-45 adapter at one end of the provided Ethernet cable into the module's Ethernet port 1.

3. Insert the RJ-45 adapter at the other end of the Ethernet cable into one of the SmartSwitch 9000's Ethernet ports.

4. Repeat steps 2 and 3 for Ethernet port 2 if you will be using a second Ethernet connection.

MOD-TAP ADAPTER

The cabling between the wall jack and the module is very important, and is also where most problems occur. The system's PRI RJ-45 adapter uses the international standard of pins 3, 4, 5, and 6 for transmit and receive. Most T1 lines in the United States and Europe use the traditional 1, 2, 4, and 5 pins. We provide an RJ-45 to RJ-45 Mod-Tap adapter that will convert between the two wiring systems.



For non-U.S. and European installations, standard cabling is sufficient (refer to following section).

MODULE TO PRI SERVICE CABLING

The PRI cabling is not included with your module. You will need to determine the length of cable you need for your connection. The PRI cabling is the same type as the Ethernet cabling: straight-through twisted-pair cable with RJ-45 adapters at each end. To complete the PRI cabling:

1. Refer to the illustration of the 9W0006-400 for the PRI ports' locations.

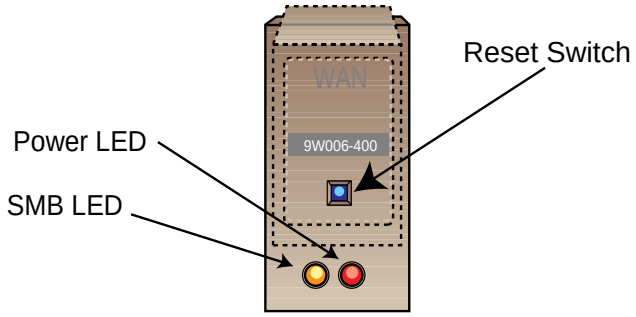
2. Insert the RJ-45 adapter at one end of the PRI cable into either the Mod-Tap adapter (U.S. and Europe) or directly into the module's PRI port 1 (for all other installations).

3. Insert the RJ-45 adapter at the other end of the PRI cable into your PRI service drop.

4. Repeat steps 2 and 3 for PRI ports 2, 3, and 4 if applicable.

RESTARTING THE SMARTSWITCH REMOTE ACCESS MODULE

The reset switch is a recessed switch located on the front panel, under the top-left plastic ejector tab as illustrated below.



The reset switch serves two functions:

1. Pressing the reset switch twice within three seconds causes the processor to reset.

2. Pressing and holding the switch on for three or more consecutive seconds causes the module to shutdown. Pressing and holding the switch again for three seconds restarts the module.

SNMP management may be used to disable this switch to enhance module security.

ACCESSING THE SMARTSWITCH REMOTE ACCESS MODULE

OVERVIEW

This chapter provides instructions for:

- accessing a SmartSwitch Remote Access Module for the first time
- remotely accessing the SmartSwitch Remote Access Module *after* the first time

Refer to the module illustration in *Hardware Overview* to help you locate the ports described in the following sections.

ACCESSING A NEW MODULE

The two methods of accessing a new module are:
- access through a PC using a terminal application
- access by Telneting to the module using the initial default IP address

Once you have used one of the two methods to access to the module, you should:
- establish an administration session with the module
- assign the module's new IP address
- access the module's release notes

For more detailed instructions, refer to the sections below.

INITIAL ASSESS USING A PC AND A TERMINAL APPLICATION

Connect one end of the supplied null modem cable to the RS232 console port on the module, and the other end of the cable to the communication port on the PC. On the PC you must then execute a communication package to emulate a terminal (VT100).

Use the following default values for your communication package:

Baud rate	9600
Parity	None
Data bits	8
Stop bits	1
Duplex	Full

After you have connection to the module, you will be ready to establish an administration session.

INITIAL ACCESS USING TELNET

You can use a remote device to the Telnet into module using the module's initial default IP address (192.186.254.254). The remote device can be a device with Telnet client software, such as a PC or a UNIX workstation, or it can be a second module or a Cabletron CyberSWITCH. Note that the modules and CyberSWITCH systems have built-in Telnet client software.

If a SmartSwitch Remote Access Module or second module is acting as the Telnet client, simply enter the following console command to Telnet into the module:

`telnet` <192.186.254.254>

Refer to the *System Commands* chapter for a complete listing of available Telnet commands.

If a remote device other than a Cabletron product is acting as the Telnet client, use the device's Telnet application to connect to the initial default IP address (192.186.254.254).

After you make a Telnet connection, you will be ready to establish an administration session (refer to the following section for instructions).

For more information on Telnet, refer to the *Remote Management* chapter.

ESTABLISHING AN ADMINISTRATION SESSION

Once you have connected to the module using either a terminal application or Telnet, you will be prompted for a login id. Enter:

admin

You will then be prompted to enter a password. All preinstalled systems are preconfigured with the same password. This is the password that is used the first time a login occurs. Being sure to enter all lowercase letters as shown below:

admin

You will now see the system prompt. We recommend that you select a new password. To do this, enter the following command at the system prompt:

pswd

Follow the onscreen instructions to change the password. Note that the password must be a 3 to 16 nonblank character string, and that it is uppercase and lowercase sensitive.

Next, follow the instructions below to assign the module's new IP address.

ASSIGNING THE MODULE'S IP ADDRESS

To assign the module's new IP address enter the following command at the system prompt:

ipconfig

As prompted, enter:

- the system's IP address
- the required subnet mask
- for the system's default route, enter the IP address of the system's default gateway (enter 0 if there is no default route)

Follow the instructions to restart the module so that the configuration changes will take effect.

Once you have assigned the module's IP address, you will Telnet into the module when you need access for functions such as system maintenance, diagnosis and verification procedures, or entering console commands.

ACCESSING THE RELEASE NOTES

The *Release Notes* provide release highlights and important information related to this release that should be reviewed before you begin the system's configuration.

The release notes are in a file called REL_NOTE.TXT. To display the release notes on the system, enter the following command at the system prompt:

[system name]> LIST REL_NOTE.TXT

REMOTE ACCESS USING TELNET

You will use Telnet to remotely access the module for routine system management once initial installation and configuration has been performed. The same instructions given in *Initial Access Using Telnet* can be followed here with one exception, instead of Telneting into the module's initial default IP address, you will Telnet to the new IP address you have configured for the module.

You will need to establish an administration session so that you can issue console commands. Once connected, you will be prompted for a login id. Enter:

admin

You will then be prompted to enter your password. If you have not yet changed the default password, enter:

admin

If you have already configured a new password, enter the new password instead.

UPGRADING SYSTEM SOFTWARE

OVERVIEW

The SmartSwitch Remote Access Module CD contains the module's upgrade software. To upgrade the module's software, you will use a device with a CD-ROM drive to Telnet into the module, then TFTP the new software files to the module.

This chapter describes how to upgrade SmartSwitch Remote Access Module system software. Instructions are included for the following software upgrade steps:

- setting up Telnet access
- TFTPing system software upgrade
- accessing Release Notes

TELNET CONNECTION

Through a remote device, you can access the SmartSwitch Remote Access Module using Telnet. To do this, the device must have Telnet client software. You will Telnet to the module's IP address. Note the initial IP address for a new module is 192.186.254.254, but you should have configured a new IP address for the module during the initial access.

Note: Do NOT place more than one SmartSwitch Remote Access Module on a LAN with the default IP address. If more than one module has the same IP address, unpredictable results will occur.

After you make a Telnet connection, enter your login id and password. Then you will be presented with a system prompt and you can enter commands at that time.

UPGRADING SOFTWARE

Perform the steps below to upgrade the module's system software:

1. Insert the 9W006/9W007 Remote Access Module CD-ROM into the PC.

2. Using the PC, Telnet to the module.

3. Once you have an administration session (you have logged in to the module) enter the special Manage Mode by typing the following command at the system prompt:

   >manage

   Note: Once Manage Mode is entered, the prompt changes from `[system name]>` to `[system name]:MANAGE>`.

4. Change the TFTP configuration by typing ***tftp change***. The following messages will be displayed:

```
Current TFTP Configuration:

The TFTP Feature is enabled.
The TFTP Client is enabled.
The TFTP Server is disabled.
```

   You will be prompted to change the status for each configuration element. Enable the TFTP Server and assign file access rights to *Admin*.

5. Use a TFTP client application to PUT the UPGRADE.OSW file from the 9W006/9W007 Remote Access Module CD-ROM to the \SYSTEM directory on the module that you want to upgrade.

6. Return to the Telnet console and issue the ***exit*** Manage Mode command.

   Note: You will receive a warning that the current configuration data has not been permanently stored in the configuration files. **Do NOT save the TFTP configuration changes.**

7. Issue the ***restart*** console command to complete the Upgrade process.

ACCESSING THE RELEASE NOTES

The *Release Notes* provide release highlights and important information related to this release that should be reviewed before you begin the system's installation and configuration.

The Release Notes located on the system's FLASH file system in a file called REL_NOTE.TXT. To display the release notes on the system, enter the following console command at the system prompt:

[system name]> LIST REL_NOTE.TXT

TROUBLESHOOTING

We include the following chapters in the *Troubleshooting* segment of the *User's Guide*:

- *System Verification*
  After your SmartSwitch Remote Access Module has been configured, and before proceeding with normal system operations, you may want to verify that the system is functional. System Verification provides instructions for verifying the system hardware and system configuration.

- *Problem Diagnosis*
  When used in conjunction with *System Verification*, this material helps diagnose problems encountered in the verification process.

- *System Messages*
  Provides a listing of all system messages, their meanings, and when applicable, possible actions you should take.

- *Trace Messages*
  For certain features you may turn a trace option on, allowing you to track system messages particular to that feature. Information is included describing how to turn the trace options on. We also list possible resulting trace messages and their meanings. The trace option is available for the following features: call trace and PPP packets.

SYSTEM VERIFICATION

OVERVIEW

After your SmartSwitch Remote Access Module has been configured, and before proceeding with normal system operation, it is necessary to verify that the system is functional. This chapter provides instructions for verifying the system hardware and system configuration.

You only need to perform the verification procedures for the options that apply to your configuration. For example, if your configuration does not use SNMP, skip the SNMP verification section.

To perform the verification procedures, WAN lines must be available and ready to use. LAN attachment components must also be available and ready to use.

During some of the procedures, we ask you to enter an administration console command. To enter these commands, you must have an active administration session. If you need instructions for starting an administration session, refer to *Accessing the SmartSwitch Remote Access Module*.

Note: At least one remote device is required to proceed with many of the verification procedures.

VERIFYING HARDWARE RESOURCES ARE OPERATIONAL

To verify the operation of the WAN and LAN hardware resources:

1. At the system prompt, enter the *dr* command to display current system messages. Determine if the WAN adapter resource is operational by viewing the system messages. At the administration console type:
   dr <return>

2. For each WAN adapter installed, look for these WAN adapter initialization messages among the system messages:

```
Bootstrap loaded on WAN card in slot <slot #>, waiting for response
Bootstrap came alive on WAN card in slot <slot #>
Downloading WAN card in slot <slot #> with operational software
Waiting for WAN card in slot <slot #> to complete initialization
WAN card in slot <slot #> signals it is operational
```

   Note: Other messages may also be displayed with the WAN adapter initialization messages.

   If you see these WAN adapter initialization messages, then the WAN adapter in the indicated slot is operational.

   If these WAN adapter initialization messages are NOT displayed for each of your WAN adapters, refer to *WAN Adapter* in the *Problem Diagnosis* chapter.

   Note: A Robbed Bit Signaling line will display a "Layer 1 up" message, but since an RBS resource does not have an ISDN layer two, a "Data link up" message will not be displayed.

3. Determine if the LAN adapter resource is operational by viewing the system messages. At the administration console type:
   dr <return>

   The *dr* command displays the current system messages. Look for these LAN adapter initialization messages among the system messages:
   ```
   LAN Adapter Reset
   LAN Adapter ROM version #.#.#
   ```

   Note: Other messages may also be displayed with the LAN adapter initialization messages.

   If these LAN adapter initialization messages are NOT displayed, refer to *LAN Adapter* in the *Problem Diagnosis* chapter.

4. If you have enabled bridging, look for these LAN adapter initialization messages among the system messages:
   ```
   LAN Port <port #> is now in the LISTENING state
   LAN Port <port #> is now in the LEARNING state
   LAN Port <port #> is now in the FORWARDING state
   ```

5. If you have enabled IP routing, look for this LAN adapter initialization message among the system messages:
   ```
   [IP] IP router is initialized successfully
   ```

   Note: Other messages may also be displayed with the LAN adapter initialization messages.

If these LAN adapter initialization messages are displayed, then the LAN adapter is operational. Proceed to the next section.

If these LAN adapter initialization messages are NOT displayed, refer to *LAN Adapter* in the *Problem Diagnosis* chapter.

VERIFYING WAN LINES ARE AVAILABLE FOR USE

To verify the availability of WAN lines, the WAN resource must already be operational. Also, the WAN lines must already be configured and connected to the SmartSwitch Remote Access Module.

To verify the availability of WAN lines:

1. Determine if WAN lines are operational by viewing the system messages. At the administration console type:
   dr <return>

   The *dr* command displays the current system messages.

2. For each primary rate line configured and attached to the SmartSwitch Remote Access Module, the following line initialization message should be displayed among the system messages:
   ```
   Data Link up: <slot #> <port #> <ces>
   ```

Depending on the resource switch type, the system will delay up to 2 minutes before attempting to bring up the data links.

Note: Other messages may also be displayed with the line initialization messages.

If this message is displayed for each configured line, then the WAN lines are available for use.

If the line initialization message for a configured line is NOT displayed, refer to *WAN Line Availability* in the *Problem Diagnosis* chapter.

VERIFYING LAN CONNECTION IS OPERATIONAL

To verify the operation of the LAN connection, the Ethernet LAN adapter resource must already be operational.

To verify the operation of the LAN connection:

1. Connect the SmartSwitch Remote Access Module to the SmartSwitch 9000's properly terminated Ethernet LAN connection.

2. Transmit a test packet onto the Ethernet LAN. At the administration console type:
   lan test <return>

   This command will display a message similar to the following:
   ```
   LAN port 1 Transmit was successful
   ```

   If the system displays this message, then the test packet was transmitted correctly.

   If this message IS NOT displayed, then the LAN connection failed. Refer to *LAN Attachment* in the *Problem Diagnosis* chapter.

VERIFYING BRIDGE IS INITIALIZED

To verify that bridging has initialized properly:

1. Determine if the bridge is in the forwarding state by viewing the system messages. At the administration console type:
   dr <return>

2. The *dr* command displays the current system messages. Look for the following LAN adapter messages among the system messages:
   ```
   LAN Port <port #> is now in the LISTENING state
   LAN Port <port #> is now in the LEARNING state
   LAN Port <port #> is now in the FORWARDING state
   ```

   Note: Other messages may also be displayed with these LAN messages.

   If you see these bridge initialization messages, then bridging is operational. If these bridge initialization messages are NOT displayed, refer to *Bridge Initialization* in the *Problem Diagnosis* chapter.

VERIFYING IP ROUTER IS INITIALIZED

To verify that IP routing has initialized properly:

1. View the system messages. At the administration console type:
   dr <return>

2. Look for the following IP message among the system messages:
   `[IP] IP router is initialized successfully`

3. For each IP interface that has been configured, the following interface initialization message should be displayed among the system messages.
   `[IP] Network initialized successfully on ddd.ddd.ddd.ddd`

   Note: Other messages may also be displayed with the IP router initialization messages.

   If you see these IP router initialization messages, then the IP router is operational. If these IP router initialization messages are NOT displayed, refer to *IP Routing Initialization* in the *Problem Diagnosis* chapter.

VERIFYING A DEDICATED CONNECTION

To verify a dedicated connection to the SmartSwitch Remote Access Module, the WAN lines that are connected to the system must be available for use, and the routing option must be properly initialized.

To verify that you have a dedicated connection:

1. View the system messages by entering the following console command:
   dr <return>

2. Look for the following system message among the displayed messages:
   `Layer 1 sync not seen - Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>`

   If the above message appears, a physical problem has been detected on the indicated line. Check for a proper connection to the SmartSwitch Remote Access Module and to the NT1 or CIU. If the NT1 or CIU appears to be functioning properly, call your carrier service and report the problem.

   If the above message does not appear in the displayed messages, proceed to the next step.

3. Look for the following system message among the displayed messages:
   `Dedicated connection to device <device name> up: Slot=<slot#>, Port=<port #>`
   If the above message is displayed, the dedicated connection is functioning.

   If the following message appears, the dedicated connection is not functioning.
   `Dedicated connection down: Slot=<slot#>, Port=<port #>`

Refer to *Remote Device Connectivity* in the *Problem Diagnosis* chapter. Because all remote devices that use dedicated connections are PPP devices, follow the described set-up procedure, then skip to the step specific for PPP devices.

VERIFYING REMOTE DEVICE CONNECTIVITY

To verify remote device connectivity to the SmartSwitch Remote Access Module, the WAN lines that are connected to the system must be available for use, and the bridging and / or routing options must be properly initialized. The remote devices must be operational and available to initiate ISDN WAN connections.

The method of connection initiation is dependent upon the remote device type. Refer to the remote device documentation to determine how to initiate an ISDN WAN connection.

To verify remote device connectivity:

1. In a controlled manner, initiate an ISDN connection from each remote device.

2. When each remote device connects to the system, it will appear as either a “REMOTE site” or as the configured Device Name (if security is enabled) on the Monitor Connections screen. To display the Monitor Connections screen, enter the following console command:
   `mc` <return>

   Note: The terminal type must be the same for Telnet and the terminal emulation. Use the `term set` administration console command to set the terminal type.

   If each remote device is able to connect to the SmartSwitch Remote Access Module, then WAN connectivity is successful.

   If a remote device is NOT able to connect to the system, then refer to *Remote Device Connectivity* in the *Problem Diagnosis* chapter.

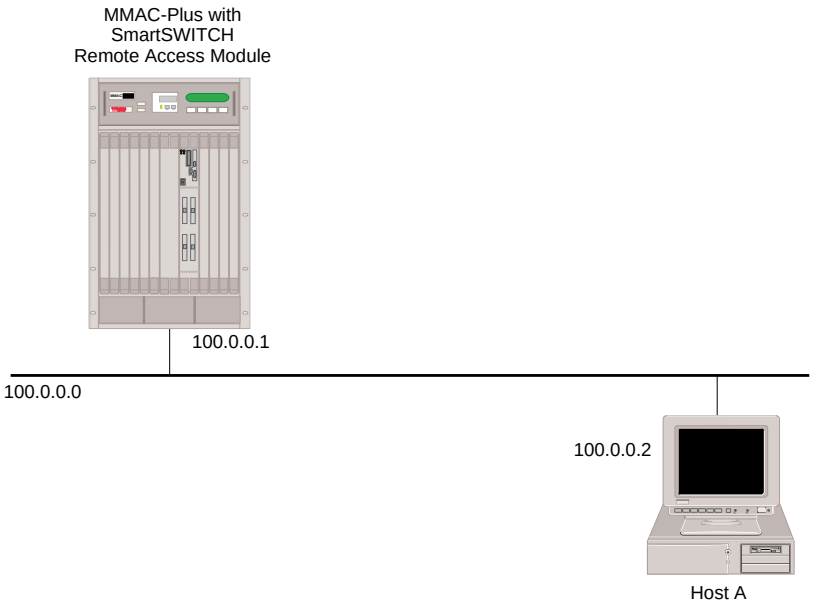
VERIFYING IP ROUTING OVER INTERFACES

The following sections provide a method of verifying that IP routing is operational over the available interfaces.

VERIFYING IP ROUTING OVER A LAN INTERFACE

To verify that IP routing is operating properly over the LAN connection, an IP host must be connected to the local LAN port on the SmartSwitch Remote Access Module. The host must be properly configured and operational on the IP network to which it is connected.

Below is an example of a configuration used to verify IP routing over a LAN connection. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you perform the IP routing verification steps.



To verify IP Routing over a LAN connection:

1. Determine if the SmartSwitch Remote Access Module can access the local IP host. On the administration console type:

   ip ping 100.0.0.2 <return>

   Issuing this command will result in a response similar to the following:

   ```
   100.000.000.002 is alive
   ```

   If the system displays this message, then IP routing over that LAN port is operational. Repeat this step for each LAN port on your Ethernet resource.

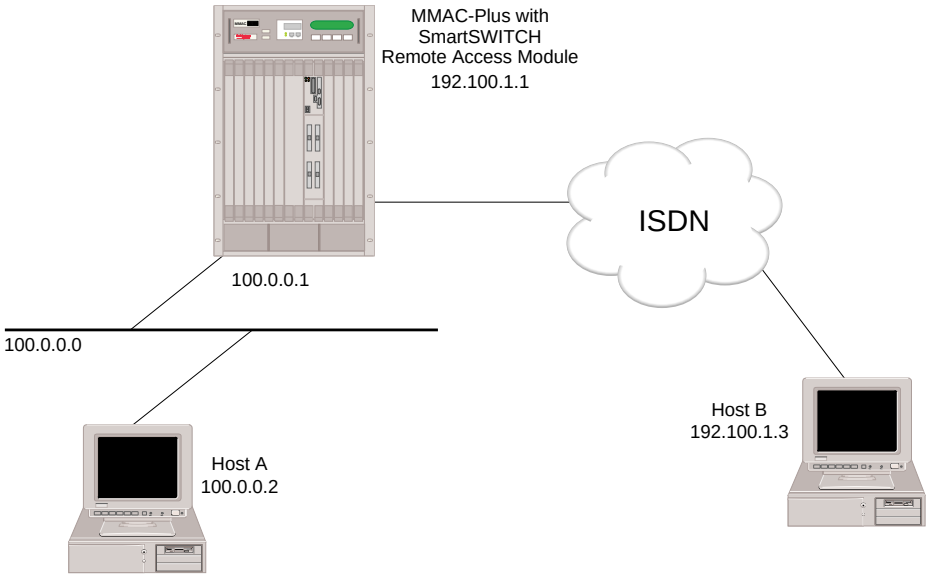
   If this message IS NOT displayed, then IP routing over the LAN connection is not operational. Refer to *IP Routing Over the LAN Connection* in the *Problem Diagnosis* chapter.

2. Once IP routing is operational on each LAN port on your Ethernet resource, then IP routing over the LAN Connection is operational.

VERIFYING IP ROUTING OVER A WAN INTERFACE

To verify that IP routing is properly operational over a WAN interface, a remote IP Host must be operational and available to initiate connections. Also, a local IP host must be connected to the local LAN port of the SmartSwitch Remote Access Module.

Below is an example of a configuration used to verify IP routing over a WAN interface. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you perform the verification steps. It also uses the "ping" command. The "ping" command sends a packet to a specified host, waits for a response, and reports success or failure. Substitute the equivalent command on your IP host.



The steps to verify the operation of IP routing over a WAN interface are:

1. Determine if a remote IP host can access the WAN interface of the SmartSwitch Remote Access Module over the WAN connection. On the remote IP host, type:
   ping 192.100.1.1 <return>

   If the remote IP host successfully pings to the SmartSwitch Remote Access Module, then continue with the next step.

   If the remote IP host CANNOT ping to the system, refer to *IP Routing Over a WAN Interface Connection* in the *Problem Diagnosis* chapter.

2. Determine if a remote IP host can access the LAN interface of the SmartSwitch Remote Access Module over the WAN connection. On the remote IP host type:
   ping 100.0.0.1 <return>

   If the remote IP host successfully pings to the SmartSwitch Remote Access Module, then continue with the next step.

   If the remote IP host CANNOT ping to the SmartSwitch Remote Access Module, refer to *IP Routing Over a WAN Interface Connection* in the *Problem Diagnosis* chapter.

3. Determine if a remote IP host can access the local IP host through the system over the WAN connection. On the remote IP host type:
   ping 100.0.0.2 <return>

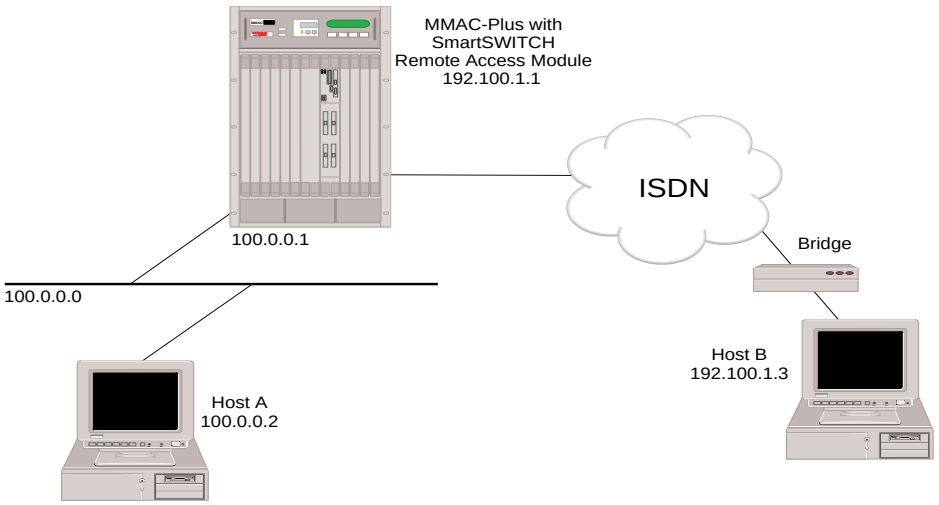
   If the remote IP host successfully pings to the local IP host, then IP routing over WAN type interface is operational. Repeat the above steps for each WAN type interface through which you wish to get access.

If the remote IP host CANNOT ping to the local IP host, refer to *IP Routing Over a WAN Interface Connection* in the *Problem Diagnosis* chapter.

VERIFYING IP ROUTING OVER A WAN REMOTE LAN INTERFACE

To verify that IP routing is properly operational over a WAN Remote LAN interface, a remote IP Host must be operational and connected to the remote LAN. The remote bridge device must be operational and available to initiate connections. Also, a local IP host must be connected to the local LAN port on the SmartSwitch Remote Access Module.

Below is an example of a configuration used to verify IP routing over a WAN Remote LAN interface. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you perform the IP routing verification steps. It also uses the "ping" command. The "ping" command sends a packet to a specified host, waits for a response, and reports success or failure. Substitute the equivalent command on your IP host.



The steps to verify the operation of IP routing over a WAN Remote LAN interface are:

1. Determine if a remote IP host can access the WAN Remote LAN interface of the SmartSwitch Remote Access Module over the WAN connection. On the remote IP host type:
   `ping 192.100.1.1` <return>

   If the remote IP host successfully pings to the SmartSwitch Remote Access Module, then continue with the next step.

   If the remote IP host CANNOT ping to the SmartSwitch Remote Access Module, refer to *IP Routing over a WAN Remote LAN Interface Connection* of the *Problem Diagnosis* chapter.

2. Determine if a remote IP host can access the LAN interface of the SmartSwitch Remote Access Module over the WAN connection. On the remote IP host type:
   `ping 100.0.0.1` <return>

If the remote IP host successfully pings to the SmartSwitch Remote Access Module, then continue with the next step.

If the remote IP host CANNOT ping to the SmartSwitch Remote Access Module, refer to *IP Routing over a WAN Remote LAN Interface Connection* of the *Problem Diagnosis* chapter.

3. Determine if a remote IP host can access the local IP host through the SmartSwitch Remote Access Module over the WAN connection. On the remote IP host type:
   `ping 100.0.0.2` <return>

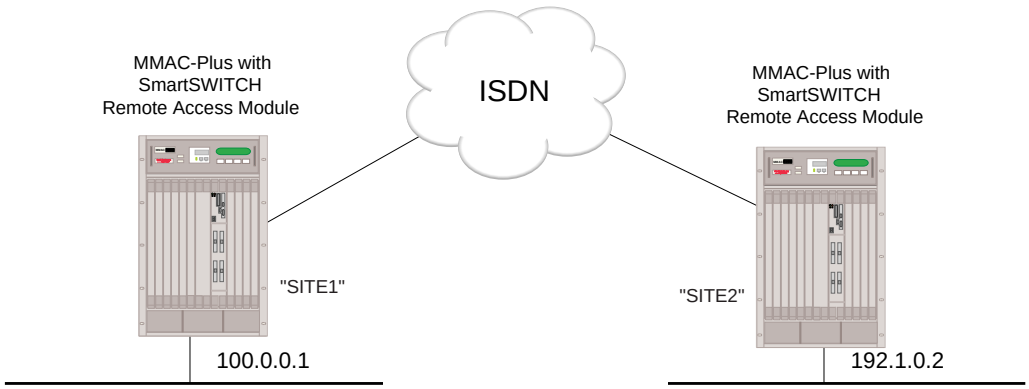
   If the remote IP host successfully pings to the local IP host, then IP routing over the WAN Remote LAN interface is operational. Repeat the above steps for each WAN Remote LAN interface through which you wish to get access.

   If the remote IP host CANNOT ping to the local IP host, refer to *IP Routing over a WAN Remote LAN Interface Connection* in the *Problem Diagnosis* chapter.

VERIFYING IP ROUTING OVER A WAN UNNUMBERED INTERFACE

To verify that IP routing is properly operational over a WAN UnNumbered interface, the SmartSwitch Remote Access Module must be operational and available to initiate connections.

Below is an example of a configuration used to verify IP routing over a WAN UnNumbered interface. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you perform the IP routing verification steps. It also uses the “ping” command. The “ping” command sends a packet to a specified host, waits for a response, and reports success or failure.



The steps to verify the operation of IP routing over a WAN UnNumbered interface are:

1. Determine if SITE1 can access SITE2 over the WAN connection. On system A type:
   `ip ping 192.1.0.2` <return>

   If the ping is successful, then continue with the next step.

   If system A CANNOT ping to system B, refer to *IP Routing over a WAN UnNumbered Interface Connection* in the *Problem Diagnosis* chapter.

2. Determine if system B can access system A over the WAN connection. On system B type:
   ip ping 100.0.0.1 <return>

   If the ping is successful, continue with the next step.

   If the system B CANNOT ping to system A, refer to *IP Routing over a WAN UnNumbered Interface Connection* in the *Problem Diagnosis* chapter.

VERIFYING IP RIP

The following sections provide a method of verifying that IP RIP is initialized, and that it is processing properly on LAN and WAN interfaces.

VERIFYING IP RIP IS INITIALIZED

Follow the steps below to verify that IP RIP processing is initialized.

1. Determine if IP RIP processing has been initialized by viewing the system messages. On the administration console type:
   dr <return>

2. The *dr* command displays the current system messages. Look for the following IP RIP message among the system message:
   `[IP RIP] RIP Protocol Initialization successful`

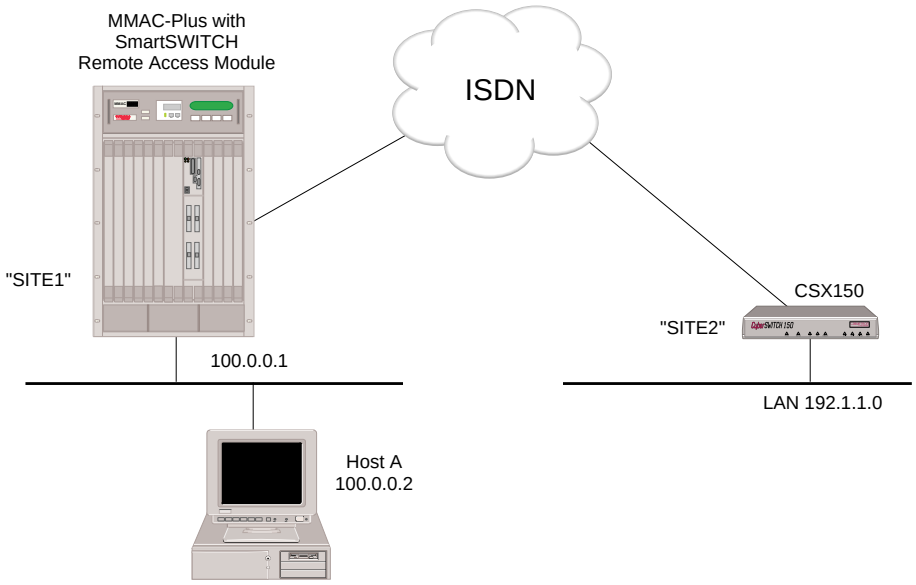
   If you see this IP RIP initialization message, the IP RIP has initialized successfully.

   If this IP RIP initialization message is NOT displayed, refer to *IP RIP Initialization* in the *Problem Diagnosis* chapter.

VERIFYING IP RIP OUTPUT PROCESSING ON A LAN INTERFACE

To verify that IP RIP Output Processing (routes advertisement) is properly operational on a LAN interface, the IP RIP processing must be successfully initialized. Also, a local IP host (router) must be connected to the local LAN port on the system and capable of learning routes information via RIP.

Below is an example of a configuration used to verify IP RIP output processing on a LAN interface. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you perform the verification steps. It also uses the *netstat* administration console command. The *netstat* command displays the IP routing table of the system. Substitute the equivalent command on your IP host.



To verify the operation of IP RIP output processing on a LAN interface:

1. Make sure that a static route to the network 192.1.1.0 is configured on SITE1. On SITE1's administration console type:

   ```
   ip route <return>
   ```

   If the route to 192.1.1.0 is displayed continue with the next step.

   If the route is NOT displayed, you will need to use SFVRA-CFG to add the static route. To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions*, then *IP Network Systems*, or click on the icon.

   c. Select *SITE1* from displayed list (you should have already configured IP subnet and network interface information for this site).

   d. Click on the *Static Routes* tab.

   e. Click on *Add*, then follow the onscreen instructions to add a static route.

   f. Download the new configuration files to SITE1.

   For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

   - For static routes: refer to *Configuring IP Network System Static Routes* in the *Configuring IP Network Information* chapter.

- For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

2. Determine if a local IP Host A has learned the route to 192.1.1.0 from System A. On IP Host A type:

   `netstat -r` <return>

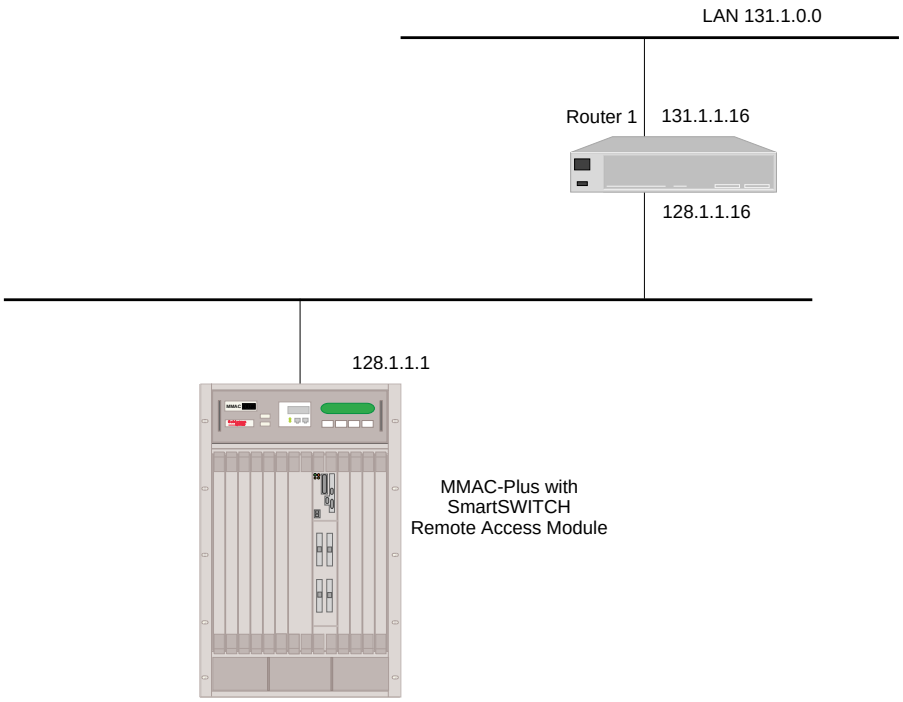
   If the route to 192.1.10 is displayed, the IP RIP output processing is operational.

   If the route is NOT displayed, refer to *IP RIP Output Processing on a LAN Interface* in the *Problem Diagnosis* chapter.

VERIFYING IP RIP INPUT PROCESSING ON A LAN INTERFACE

To verify that IP RIP Input Processing (routes learning) is properly operational on a LAN interface, IP RIP processing must be successfully initialized. Also, a local IP router must be connected to the local LAN port on the system and capable of propagating routes information via RIP.

Below is an example of a configuration used to verify IP RIP input processing on a LAN interface. It uses IP addresses specified to the example. Substitute the IP addresses of your network when you perform the verification steps. It also uses the `netstat` command. The `netstat` command displays the IP routing table of the system. Substitute the equivalent command on your IP router.



To verify the operation of IP RIP input processing on a LAN interface:

1. Determine if the SmartSwitch Remote Access Module has learned the route to 131.1.0.0 from Router 1. On the administration console type:
   ip route <return>

   If the following route entry is displayed among other route entries, the IP RIP input processing is operational. The 'P' (Protocol) field should have 'R', which indicates that the entry was learned via RIP.

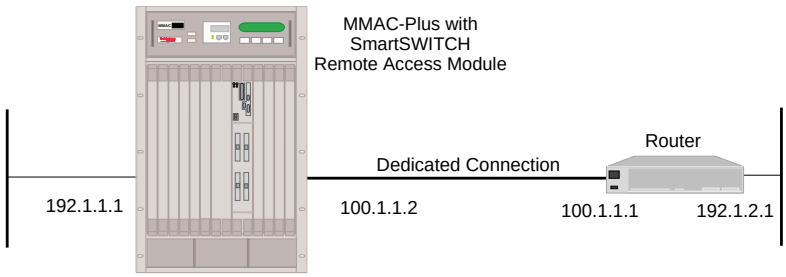
```
Destination      Subnet-Mask      Next Hop      Mtr T/P TTL IF AGE
131.1.0.0        255.255.0.0      128.1.1.16     1   R/R 999   n nnn
```

2. If the route is NOT displayed, refer to *IP RIP Input Processing on a LAN Interface* in the *Problem Diagnosis* chapter.

VERIFYING IP RIP OUTPUT PROCESSING ON A WAN INTERFACE

To verify that IP RIP Output Processing (routes advertisement) is properly operational on a WAN interface, the IP RIP processing must be successfully initialized.

Below is an example of a configuration used to verify IP RIP output processing on a WAN interface. It uses IP addresses specific to the example. Substitute the IP addresses of your network when you perform the verification steps. It also uses the *show ip route* command. The *show ip route* command is used by a specific router to display the IP routing table. Substitute the equivalent command for your IP router.



The steps to verify the operation of IP RIP output processing on a WAN interface are:

1. Make sure that a dedicated connection between system and Router is up and operational. On the system's administration console:
   Type: *cs*<return>

   If the connection to Router is displayed, the continue with the next step.

2. Determine if Router has learned the route to 192.1.1.0 from the system. On the Router:
   Type: *show ip route*<return>

   If the route to 192.1.1.0 is displayed, the IP RIP output processing is operational.

   If the route is NOT displayed, refer to *IP RIP Output Processing on a WAN Interface* in the *Problem Diagnosis* chapter.

VERIFY IP RIP INPUT PROCESSING OPERATIONAL ON A WAN INTERFACE

To verify that IP RIP Input Processing (routes learning) is properly operational on a WAN interface, the IP RIP processing must be successfully initialized.

The same example that is used in the previous section is used to verify IP RIP input processing on a WAN interface.

To verify the operation of IP RIP Input processing on a WAN interface:

1. Make sure that a dedicated connection between system and Router is up and operational. On the SmartSwitch Remote Access Module administration console:
   Type: *cs*<return>

   If the connection to Router is displayed, the continue with the next step.

2. Determine if system has learned the route to 192.1.2.0 from the Router. On the SmartSwitch Remote Access Module administration console:
   Type: *ip route*<return>

   If the route to 192.1.2.0 is displayed, the IP RIP input processing is operational.

   If the route is NOT displayed, refer to *IP RIP Input Processing on a WAN Interface* in the *Problem Diagnosis* chapter.

VERIFYING IPX ROUTER IS INITIALIZED

To verify that the IPX Routing option has initialized properly.

1. Determine if IPX routing has been initialized on the SmartSwitch Remote Access Module by viewing the system messages. To display the messages enter the following console command:
   dr <return>

2. Look for the following IPX message among the system messages:
   `[IPX] IPX router is initialized successfully`

   Also, for each IPX interface that has been configured, the following interface initialization message should be displayed among the system messages.
   `[IPX] Network initialized successfully on xxxxxxxx:xxxxxxxxxxxx`

   Note: Other messages may also be displayed with the IPX router initialization messages.

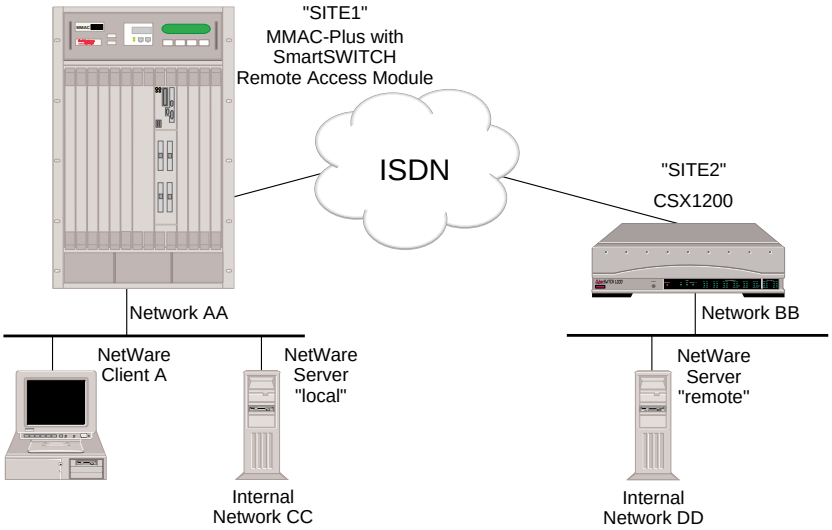
   If you see these IPX router initialization messages, the IPX router is initialized.

   If these IPX router initialization messages are NOT displayed, refer to *IPX Routing Initialization* in the *Problem Diagnosis* chapter.

VERIFYING IPX ROUTING IS OPERATIONAL

To verify that IPX routing feature is properly operational, a local NetWare client, a local NetWare server and a remote NetWare server must be operational.

The following graphic illustrates an example network we will use to describe how to verify that IPX routing is operational. It uses IPX network addresses specific to the example. Substitute the IPX network numbers of your network when you perform the verification steps. The example also uses NetWare commands available for the Windows 95 workstation. Substitute the equivalent commands on your NetWare client.



VERIFYING IPX ROUTING OVER A LAN CONNECTION

To verify the operation of IPX Routing over a LAN connection:

1. Determine if SITE1 can access the local NetWare Server “local.” On SITE1’s administration console type:

   ```
   ipx diag cc:1 <return>
   ```

   Note: Node address 1 is used by the NetWare servers as part of their internal address.

2. If the system displays a response to the *ipx diag* command similar to:

   ```
   received 3 components from cc:1
   ```

   then IPX routing over that LAN port is operational.

   If this message IS NOT displayed, then IPX routing over the LAN connection is not operational. Refer to *IPX Routing over the LAN Connection* in the *Problem Diagnosis* chapter.

VERIFYING AN IPX REMOTE LAN CONNECTION

To verify that IPX routing is properly operating over a WAN Remote LAN interface, a remote IPX router (in our example this is SITE1) must be operational and connected to the Remote LAN. The remote bridge device (in our example, this is SITE2) must be operational and available to initiate connections.

1. From the router (SITE1), verify that the IPX Remote LAN interface has initialized. On the router's administration console type:
   ```
   dr
   ```
   You should see messages stating that the IPX network has initialized successfully on *xxxx*. Verify that "*xxxx*" is the network number of the Remote LAN.

2. Determine the router's (SITE1) MAC address. From the router, issue the command:
   ```
   ver
   ```

3. From the remote bridge (SITE2), attempt to access the IPX router by issuing the following administration console command:
   ```
   ipx diag xxxx:yyyyyyyyyyyy
   ```
   where: *xxxx* is the IPX Network Number
   yyyyyyyyyyyy is the router's MAC address

4. Verify the call has come up. From the router side (SITE1), issue the following administration console command to display the monitor connections screen:
   ```
   mc
   ```
   If the call is displayed on the monitor connections screen, the IPX Remote LAN interface is operational. If the call is not displayed, refer to *IPX Routing over the Remote LAN Connection* in the *Problem Diagnosis* chapter.

VERIFYING IPX ROUTING OVER A WAN CONNECTION

To verify the operation of IPX Routing over a WAN connection:

1. Determine if NetWare Client A can see the remote NetWare Server "remote." To do this, activate NetWare Client A's desktop network neighborhood feature. Then check to see if "remote" is included in Client A's network neighborhood.

2. If "remote" is included in Client A's network neighborhood, them IPX over the WAN connection is operational. If it does not appear in the network neighborhood, then IPX over the WAN connection is not operational. Refer to *IPX Routing Over the WAN Connection* in the *Problem Diagnosis* chapter.

VERIFYING TRIGGERED RIP/SAP

Verify whether or not triggered RIP / SAP has started and is operational:

1. Determine if triggered RIP / SAP has started by viewing the system messages. To display the messages, enter the following console command:
   dr <RET>

2. Look for following message among the system messages:
   `Starting Triggered RIP/SAP for <WAN Peer>`

3. If this message is displayed, continue check to see if Triggered RIP / SAP is operational. If message is not displayed, refer to *Triggered RIP/SAP Start Up*.

4. Determine if triggered RIP is operational. On the administration console, type:
   ipx trigrip stats

5. Examine statistics for activity. Refer to *Triggered RIP Statistics* for possible statistics and their descriptions.

6. Create a change in the route (for example, shut down a server). Again examine statistics (*ipx trigrip stats)* to verify the change is propagated to other side.

7. If statistics do not reflect change, refer to *Triggered RIP/SAP Operation*.

8. Repeat process (beginning at step 4) for SAP, but substitute the following console command:
   ipx trigsap stats

VERIFYING THE APPLETALK ROUTING FEATURE

VERIFYING APPLETALK ROUTING IS INITIALIZED

1. Determine if AppleTalk routing has been initialized on the SmartSwitch Remote Access Module by viewing the system messages. To view the system messages, enter the following console command:
   dr

2. Look for the following message among the system messages:
   `AppleTalk routing initialized successfully`

3. For the AppleTalk port that has been configured, the following port initialization message should be displayed among the system messages:
   `AppleTalk successfully initialized on <port-type> with address <net.node>`

   Note: <port-type> is either LAN port 1, LAN port 2 or WAN.
   <net.node> is the AppleTalk address assigned to this port.

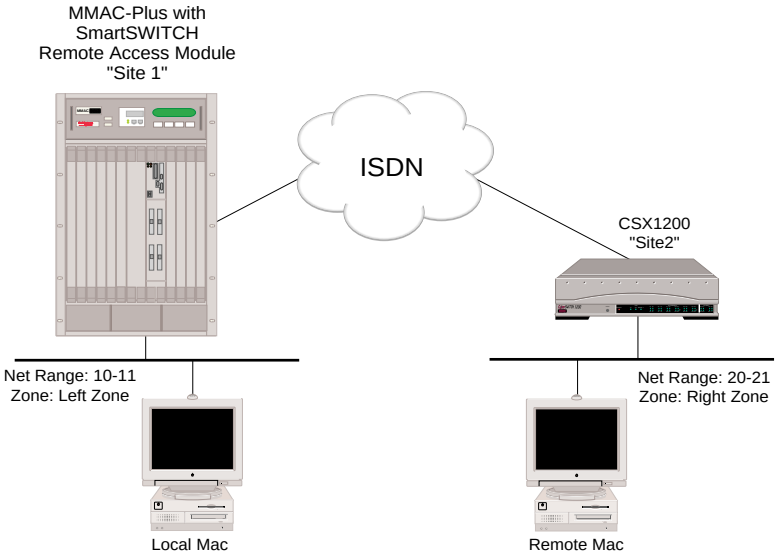
4. If you see these AppleTalk routing initialization messages, then the AppleTalk routing has initialized properly.

If these messages are NOT displayed, refer to *AppleTalk Routing Initialization* in the *Problem Diagnosis* chapter.

VERIFYING APPLETALK ROUTING IS OPERATIONAL

To verify that AppleTalk routing is properly operational, a remote Macintosh must be operational and available to initiate WAN connections via a remote AppleTalk router device. Also, a local Macintosh device must be connected to the local LAN port on the SmartSwitch Remote Access Module.

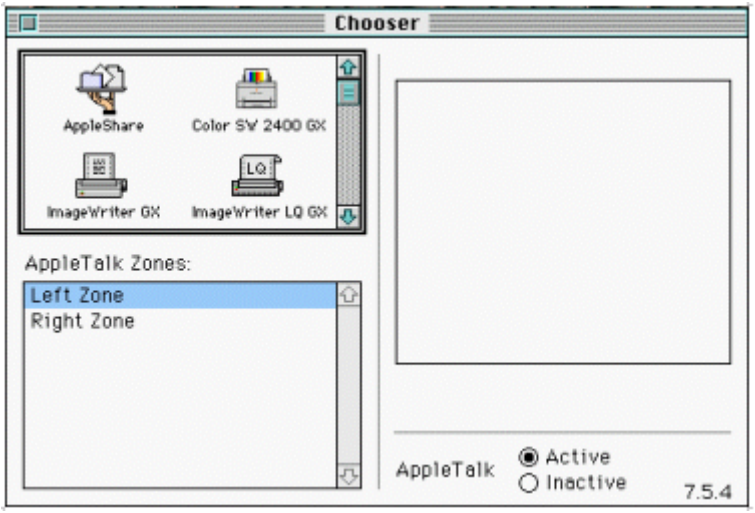
Below is an example of a configuration used to verify AppleTalk Routing operation. It uses AppleTalk addresses, zones and resource names specific to the example. Substitute those of your network when you perform the AppleTalk Routing feature verification steps.



VERIFYING APPLETALK ROUTING OPERATIONAL OVER THE LAN CONNECTION

The steps to verify the operation of AppleTalk Routing feature over a LAN connection are:

1. Determine if the local Macintosh can see all zones. Bring up the Chooser on the Local Mac:



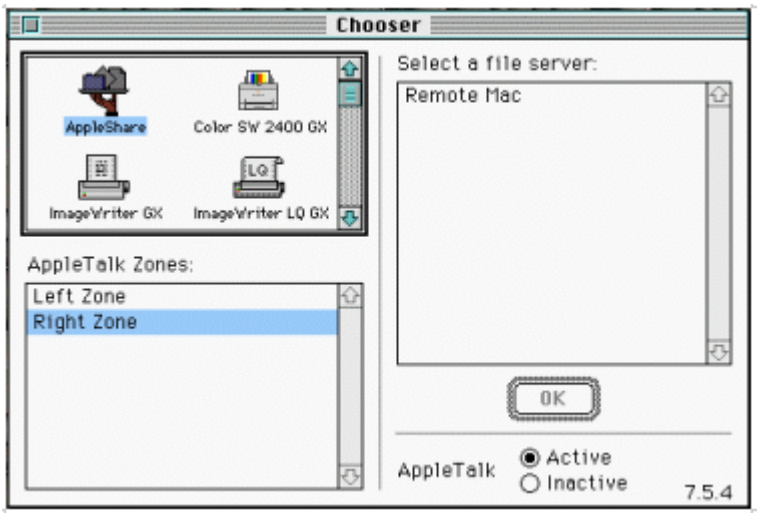
2. If a list of all zones (*Left Zone* and *Right Zone*) appear in the Chooser as shown above, then the AppleTalk Routing over a LAN connection is operational. Continue with the next step.

3. If all zones are NOT displayed, then AppleTalk Routing over the LAN connection is not operational. Refer to *AppleTalk Routing Operation over the LAN Connection* in the *Problem Diagnosis* chapter.

VERIFYING APPLETALK ROUTING OPERATION OVER A WAN CONNECTION

The steps to verify the operation of AppleTalk Routing feature over a WAN connection are:

1. Determine if the Local Mac can access the Remote Mac. On the Local Mac, in the Chooser, pick AppleShare on *Right Zone*:



2. If Remote Mac appears in *Select a file server:* box, then AppleTalk Routing over the WAN connection is operational.

3. If Remote Mac IS NOT displayed, then AppleTalk Routing feature over the WAN connection is not operational. Refer to *AppleTalk Routing Operation Over the WAN Connection* in the *Problem Diagnosis* chapter.

VERIFYING SNMP IS OPERATIONAL

1. To verify that the SNMP feature is operational, enter the `snmp stats` command at the administration console. If the statistics display appears, the SNMP subsystem should be fully operational. If the following message is displayed, SNMP is not operational:

   ```
   SNMP is not enabled
   ```

   If the preceding message is displayed, refer to *SNMP* in the *Problem Diagnosis* chapter for possible actions you may take to make the SNMP feature operational.

2. To verify that the MIB objects can be retrieved via the SNMP get command, begin by making sure that the latest version of the enterprise MIB (the ih_mib.asn file) has been compiled at the desired SNMP network management station(s). Once the new version of the MIB is compiled, you can issue the SNMP get command.

3. To verify the SmartSwitch Remote Access Module SNMP Agent is returning the correct values, it is possible to compare the values of the MIB objects retrieved via the SNMP get command to the output available via various system administration console and dynamic management commands. For example, the `isdn usage` console command displays B-channel information. This information corresponds to the MIB isdnUsageMonitor group objects, a subset of the ihSystemMonitor group. The `dr` console command will return output that contains information that corresponds to the MIB ihStatusReport table. Other console commands that will output information that includes values that correspond to MIB objects are `ds`, `udp stats`, `ip stats`, and `snmp stats`.

VERIFYING THE DIAL OUT FEATURE

To perform the Dial Out verification for a remote device, you need to know the configured device name associated with the device's device table entry. Note that the device name is case sensitive.

1. The following administrative command is used to verify that the Dial Out feature is operational to a specific remote device:
   `call device <device name>`

   For example, to verify that the Dial Out feature is operational for remote device with fred as the configured device name, you would enter `call device fred` at the system prompt.

2. A message will be displayed indicating whether or not the call was made successfully. Refer to *Dial Out* in the *Problem Diagnosis* chapter if the call was not made successfully.

VERIFYING COMPRESSION IS OPERATIONAL

1. Make sure compression is enabled on a system-wide basis.

2. Cause a call to be established with a device for which per-device compression is enabled.

3. To verify that compression is in effect with the device, issue the `cmp stats <devicename>` console command while the connection is in place. If compression is in effect, this command will display the current compression counters and ratios. If compression is not in effect, the command will return an indication that the device is a non-compressed connection. If compression is not in effect, refer to *Compression* in the *Problem Diagnosis* chapter.

VERIFYING RESERVED BANDWIDTH IS OPERATIONAL

1. Configure several different combinations of lines and devices.

2. Attempt outbound and inbound calls.

3. Verify the proper success and reject of each.

   If there is a problem, check the configuration of the profiles and how they are assigned to each device. Use SFVRA-CFG to check the profile configurations. To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions* then select *Sites*, or click the icon.

   c. Select a site from the displayed list.

   d. Click on the *Systems* tab.

   e. Click on *Edit Systems Settings*.

   f. Click on the *Circuit Groups* tab.

   g. Check the circuit group configuration for this device. Make any necessary changes.

h. Repeat steps *c* through *g* for each additional site you want to check.

i. If you make any changes, you will need to download the new configuration files to the effected sites.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For profiles: refer to *Configuring the Site's Systems* in the *Configuring Sites* chapter.
- For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

VERIFYING A SEMIPERMANENT CONNECTION

Follow the same procedure outlined in the *dial out verification* section. If you can successfully use the call device command to call the device assigned to the semipermanent connection, then the connection is working. If not, follow the instructions actions in the dial out verification section.

PROBLEM DIAGNOSIS

OVERVIEW

This chapter, when used in conjunction with the *System Verification* chapter, helps diagnose and correct problems encountered in the verification process.

During some of the diagnosis procedures, we ask you to enter an administration console command. To enter these commands, you must have an active administration session. If you need instructions for starting an administration session, refer to *Accessing the SmartSwitch Remote Access Module*.

WAN ADAPTER

Problem:
The system does not display the WAN Adapter Initialization messages. Instead, the system displays one of the following messages:

```
Error mapping WAN adapter # into Host memory map
Type mismatch of configured & installed adapter #
Error initializing WAN card: #
Failure during static RAM test on adapter #
Error downloading operational software to adapter #
Error downloading bootstrap program to adapter #
```

Action:

1. Note the displayed error message. Restart the SmartSwitch Remote Access Module, and recheck for one of the above error messages.

2. If the error message is still displayed, contact Customer Support.

LAN ADAPTER

Problem:
The system does not display the LAN Adapter Initialization messages. Instead, the system displays one of the following messages:

```
Invalid LAN Adapter identifier
LAN Adapter Command Timeout
LAN Adapter FIFO not empty, status = #
LAN Adapter LAN Controller error
LAN Adapter Response Timeout
MAC layer Bridge did not Initialize
[IP] Initialization failure
```

Action:

1. Note the displayed error message. Restart the SmartSwitch Remote Access Module, and recheck for one of the above error messages.

2. If the error message is still displayed, contact your distributor for hardware replacement.

BRIDGE INITIALIZATION

Problem:
The system does not display the following bridge initialization messages:

```
LAN Port <port #> is now in the LISTENING state
LAN Port <port #> is now in the LEARNING state
LAN Port <port #> is now in the FORWARDING state
```

Action:

1. Make sure the *LAN Adapter* has initialized correctly.

2. Using SFVRA-CFG, check the configuration to verify the bridge is enabled. To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions* then select *Sites* or click the icon.

   c. From the displayed list, double click on the site in question.

   d. Click on the *Systems* tab.

   e. Select the system in question, then click on *Edit System Settings.*

   f. Under *Bridging* information, check to make sure that a check appears next to *Enable* (bridging information is included under the *Properties* tab).

   g. If you made a change, download the new configuration files to effected site.

   For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

   - For enabling bridging: refer to *Configuring the Site's Systems* in the *Configuring Sites* chapter.
   - For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

IP ROUTING INITIALIZATION

Problem:
The system does not display the expected IP routing initialization messages.

Action:

1. If you did not see the following IP message:

   ```
   [IP] IP router is initialized successfully
   ```

   Using SFVRA-CFG, check the configuration to verify that IP routing is enabled. To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions* then select *Sites* or click the icon.

c. From the displayed list, double click on the site you are diagnosing.

d. Click on the *Systems* tab.

e. Select the system in question then click on *Edit System Settings.*

f. Under the IP information, check to make sure that a check appears next to *Enable* (IP information is included under the *Properties* tab).

g. If you made a change, download the new configuration files to effected site.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For enabling IP routing: refer to *Configuring the Site's Systems* in the *Configuring Sites* chapter.
- For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

2. The failure to see the following IP message for each IP interface:

```
[IP] Network initialized successfully on ddd.ddd.ddd.ddd
```

indicates that you may have either not configured a needed interface or have incorrectly configured an interface. Check the system's IP network interface configuration using SFVRA-CFG. If there are any problems, make the necessary corrections. To do this:

a. If it is not already running, start up SFVRA-CFG.

b. From the toolbar, select *Functions*, then *IP Network*, then *Systems*, or click on the icon.

c. Select the system's site from displayed list.

d. Click on the *Network Interface* tab.

e. Add any missing interfaces and / or make any necessary corrections to existing interfaces.

f. If you made any changes, download the updated configuration files to the effected system.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For network interfaces: refer to *Configuring IP Network System Interfaces* in the *Configuring IP Network Information* chapter.
- For downloading updated configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

WAN LINE AVAILABILITY

Problem:
The system does not display the WAN line availability messages. Instead, the system displays the following message after the ***status*** console command is issued:

```
Line (slot #, port #) down
```

Action:
1. Verify that the line is correctly attached to the proper system resource and port.

2. If the line was correctly attached in action 1, try restarting the system.

3. If actions 1 and 2 fail to correct the problem, call your phone company (carrier) to check the status of the line.

Problem:
The system does not display the WAN line availability messages. Instead, the system displays the following message after the ***status*** console command is issued:

```
Out Svc 1 (slot #, port #)
```

This means that Layer 1 cannot be established, most likely due to WAN cabling problems.

Action:
1. If the system has been operational for longer than 2 minutes, verify that the line is correctly attached to the proper system resource and port. If not, wait for 2 minutes and check again for the WAN line availability messages.

2. If using a NT1 or CSU, examine the local and network lights of the NT1 or CSU. If the local light is on, try another cable between the SmartSwitch Remote Access Module and the NT1 or CSU. If the local light is not on, but the network error light is on, contact your line provider.

3. If the line was correctly attached in action 1, turn the system off, then on. If this fails to correct the problem, continue with the next step.

4. Refer to the *Ordering ISDN Service* chapter. Compare the parameters with those required by the PRI line provider. It is possible that there is a mismatch.

5. If the above actions fail to correct the problem, then call your phone company (carrier) to check the status of the line. If it is determined that there is no problem with the line, contact Customer Support.

Problem:
The system does not display the WAN line availability messages. Instead, the system displays the following message after the ***status*** console command is issued:

```
Out Svc (2, 3, 4, or 5) (slot #, port #)
```

These mean that Layer 2 cannot be established, most likely due to an invalid configuration.

Action:

1. If the system has been operational for longer than 2 minutes, verify that the line is correctly attached to the proper system resource and port. If not, wait for 2 minutes and check again for the WAN line availability messages.

2. If the line was correctly attached in action 1, turn the system off, then on. If this fails to correct the problem, continue with the next step.

3. For the "Out Svc2 (slot #, port #)" message with a Primary Rate line, call your line provider and have the data link restarted.

4. For the "Out Svc3 (slot #, port #)" on an Auto TEI line, check configuration. Try reconfiguring (using SFVRA-CFG) the line using non-auto TEI. To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions*, then select *Circuits* or click the icon.

   c. From the displayed list, double click on the circuit (line) in question.

   d. Click on the *Data Link* tab.

   e. Change the TEI negotiation value from *Auto* to *Non-Auto*. Click *OK*, then click *Close*.

   f. If you made any changes to the configuration, download the new configuration files to effected site.

   For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

   - For data links: refer to *Configuring Circuit Data Links* in the *Configuring Circuits* chapter.

   - For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

5. If the above actions fail to correct the problem, then call your phone company (carrier) to check the status of the line. If it is determined that there is no problem with the line, contact Customer Support.

Problem:

A WAN line is unavailable, and the following two messages are displayed together (to display messages, issue the *dr* console command):

```
WAN card in slot <slot #> signals it is operational
Abnormal response rcvd: state=-1 msg=73 reason=6 cc state=-1
```

Action:

1. Check the configuration. Verify that all lines are configured with corresponding data links. If this is not the case, add data links to all configured lines using *SFVRA-CFG*.To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions*, then select *Circuits* or click the icon.

c. From the displayed list, double click on a circuit (line).

d. Click on the *Data Link* tab.

e. Check the data link information. Make corrections as required.

f. If you made any changes to the configuration, download the new configuration files to effected site.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For data links: refer to *Configuring Circuit Data Links* in the *Configuring Circuits* chapter.
- For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

DEDICATED CONNECTIONS

Problem:
A dedicated connection is not functioning.

Action:
If the dedicated connection is not up, this usually indicates that the device could not be validated for some reason. Check the configuration for the device that will be using the dedicated connection, and make any necessary corrections.

REMOTE DEVICE CONNECTIVITY

Problem:
A remote device is not able to connect to the SmartSwitch Remote Access Module.

Set-up:
The system software should be up and running. (At the administration console: if you are in the Connection Monitor window, exit to the "[`System Name`] >" prompt.)

1. Enable the call trace messages with the *`trace on`* console command.
2. Erase the current system messages using the *`er`* console command.
3. In a controlled manner, initiate an ISDN connection from the remote device.

Action:
1. After a connection has been initiated, view the system messages (display system messages by issuing the *`dr`* console command). Look for the following call request messages among the system messages:

```
In - INCOMING CALL Call Id=<call Id> Slot =<slot #> Port=<port #> Chans=<bearer
channel map> Ces=<comm endpoint suffix> Rate=<data rate>
```

```
Out - CONNECT Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer
channel map> Ces=<communication endpoint suffix> ConnId=<connect Id>
In - CONNECT Call Id=<call Id> Slot=<slot#> Port=<port #> Chans=<bearer channel
map> Ces=<communication endpoint suffix> ConnId=<connect Id>
```

If the system reports these messages, then continue with the next step.

If the system does *not* report these messages, the remote device is not correctly connecting to the system. Check and verify the configuration of the remote device.

2. If the system displays the following message among the system messages (display system messages by issuing the *dr* console command),
   ```
   Security Rejection-Invalid Calling Line Id - <#>
   ```
   the network is indicating a calling line identifier that is not configured for any valid device in the system Device list. The number "#" indicates the actual number presented by the network.

3. For Remote Bridge Devices:
   If the system displays the following messages among the system messages,
   ```
   Security Rejection - Caller did not negotiate security
   Security Rejection - No Bridge Address given by caller
   Security Rejection - Unknown Calling Bridge
   Security Rejection - No Password given by caller
   Security Rejection - Invalid Password given
   Security Rejection - HDLC not supported by the caller
   ```
   review the system configuration for the remote device. You can also refer to the *System Messages* chapter for the message meanings and the appropriate actions to be taken.

4. For IP Host Devices:
   If the system displays the following messages among the system messages:
   ```
   IP Call Dropped: ID_RSP was not received from remote
   IP Call Dropped: XID was not received from remote
   IP Security Rejection - Digit string wrong length
   IP Security Rejection - Invalid Security ID <Id string>
   ```

   Review the system configuration for the remote device. You can also refer to the *System Messages* chapter for the message meanings and the appropriate actions to be taken. The first two messages indicate that the system did not receive the required protocol data. The second two messages indicate that the security configuration is incorrect.

5. For PPP Devices:
   If the system displays any error or warning messages that begin with the following prefixes:
   ```
   [PAP].....
   [CHAP].....
   [AUTH].....
   ```

   There probably is an error in the remote device configuration. Review your remote device configuration. You can also refer to the *System Messages* chapter for the message meanings and the appropriate actions to be taken.

LAN ATTACHMENT

Problem:
The LAN TEST command displays the following message:

```
LAN port 1 Transmit was not successful
```

Action:

1. Check to see if the Ethernet LAN is properly connected to the SmartSwitch Remote Access Module.

2. Check to see if the Ethernet LAN is properly terminated.
   (Test: Can any other machine transmit data successfully onto this LAN?)

3. If the problem is still not resolved, contact Customer Support.

IP ROUTING OVER INTERFACE CONNECTIONS

This section provides diagnostic information for IP routing over various interface connections.

IP ROUTING OVER THE LAN INTERFACE CONNECTION

Problem:
The system does not display the correct message after the ping command. Instead, the system displays the following message:

```
No response from <ip-address>
```

Action:

1. Verify that the routing entry for the destination network exists by entering the following administrative console command:

   ```
   iproute <ip-address>
   ```

   If the command returns "`No route is available for <ip-address>`", the routing entry does not exist. To correct, add the routing entry using *SFVRA-CFG*. To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions*, then *IP Network*, then *Systems*, or click on the icon.

   c. Select the system's site from displayed list (you should have already configured IP subnet and network interface information for this site).

   d. Click on the *Static Routes* tab.

   e. Click on *Add*, then follow the onscreen instructions to add a static route.

   f. Download the new configuration files to the site.

   For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For static routes: refer to *Configuring IP Network System Static Routes* in the *Configuring IP Network Information* chapter.

- For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

2. Check that the system and the specified Host both have the same Subnet mask and Sub network number for that IP address using SFVRA-CFG. Correct the Host configuration, or the system configuration as required. To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions* then click on *IP Network*, then on *Subnets*, or click on the toolbar.

   c. Double click on the particular subnet that applies to the system.

   d. Check the subnet's mask and network number. Compare the values to the host's configuration.

      If you change the system's mask and / or subnetwork number instead of the host's, you will need to configure a new subnet, and associate the system with the new subnet. This is because you cannot change these values for the subnet once it has been configured. Refer to the SFVRA-CFG documentation if you need to do this.

   For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

   - For static routes: refer to *Configuring IP Network Subnet Information* in the *Configuring IP Network Information* chapter.

   - For downloading updated configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

3. Verify that the ARP entry for the specified IP address exists. As required, ping from the IP Host so that the ARP entry is updated. Use the `ip arp` console command to look at the ARP cache entries. If the ARP cache entry for the Host does not exist, verify that the Host is operational and that the SmartSwitch Remote Access Module and the Host are both physically connected to the same LAN segment.

4. If the ARP cache entry exists for the Host, check that the IP Host has the same encapsulation type as the SmartSwitch Remote Access Module. The system can receive and recognize either Ethernet or SNAP type encapsulations. Correct the IP Host or system configuration (through SFVRA-CFG*)* for encapsulation type. To do this for SmartSwitch Remote Access Module:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions* then click on *IP Network*, then on *Subnets*, or click on the toolbar.

   c. Double click on the particular subnet that applies to the system.

d. Click on the *Network Interfaces* tab.

e. Double click on the interface in question.

f. Click on the Expert Properties tab.

g. Check the value for the Packet Encapsulation type. Compare the value to the host's value. If they are not the same, change the value to make them the same.

h. If you made any changes, download the new configuration files to the site.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For static routes: refer to *Configuring IP Network Subnet Interfaces* in the *Configuring IP Network Information* chapter.
- For downloading updated configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

5. Try to ping the Host from another device on the LAN. If this is also unsuccessful, this may indicate a problem with the Host.

6. Verify that the hardware address (MAC address) for the IP Host in the system's ARP cache is correct. If it is not correct, verify the configuration in the IP Host.

IP Routing Over a WAN Interface Connection

Problem:
The remote IP Host connected to a WAN interface does not receive a ping response from the SmartSwitch Remote Access Module WAN interface.

Action:
1. Verify that the WAN connection is up. Use the *mc* console command to display the Connection Monitor display. Check for the connection. If the connection is up, continue with the next step.

   If the connection is not up, refer to the section titled *Remote Device Connectivity*.

2. Verify that the WAN interface is properly initialized. Use SFVRA-CFG to check for the proper WAN interface (refer to page 77 for instructions). If it exists, continue with the next step.

   If the proper WAN interface does not exist, make corrections to the system configuration using SFVRA-CFG.

3. Check that the IP address configured for the IP Host device matches the address configured on the IP Host device. Make corrections to the SmartSwitch Remote Access Module's configuration (using SFVRA-CFG), or to the IP Host's configuration, as required. To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions*, then *IP Network*, then *Systems*, or click on the icon.

c. Select the IP Host's site from displayed list (you should have already configured IP subnet and network interface information for this site).

d. Click on the *Network Interfaces* tab.

e. On the resulting screen, check the IP Host's IP address. Compare it to the address configured on the IP host (for the IP host). If these are not the same, make corrections where necessary.

f. If you made a change using SFVRA-CFG, download the updated configuration files to the site.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For network interfaces: refer to *Configuring IP Network System Interfaces* in the *Configuring IP Network Information* chapter.
- For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

Problem:
The remote IP Host connected to a WAN interface on the SmartSwitch Remote Access Module does not receive a ping response from the LAN interface.

Action:
1. Verify that the remote IP Host can access the WAN interface of the SmartSwitch Remote Access Module. If the remote IP Host accesses the WAN interface successfully, then continue with the next step.

   If the remote IP Host is not able to access the WAN interface, then refer to the preceding problem and associated actions.

2. Verify that the LAN interface is properly configured by using SFVRA-CFG (refer to page 77 for instructions). If the proper LAN interface exists, then continue with the next step.

   If the proper LAN interface does not exist, use SFVRA-CFG to make the necessary corrections.

3. Verify that the remote IP Host is initiating a call to the SmartSwitch Remote Access Module. Since the LAN interface has an IP address assigned with a different network number than the one for the remote IP Host, the remote IP Host may need a proper route entry for the local network where the SmartSwitch Remote Access Module is located. Make corrections to the remote IP Host configuration.

Problem:
The remote IP Host connected to a WAN interface on the SmartSwitch Remote Access Module does not receive a ping response from the local IP Host.

Action:
1. Verify that the remote IP Host can access the LAN interface of the SmartSwitch Remote Access Module. If the remote IP Host accesses the LAN interface, then continue with the next step.

If the remote Host is unable to access the LAN interface, refer to the preceding problem and associated actions.

2. Verify that the local IP Host has the route entry for the remote network with the SmartSwitch Remote Access Module as the next hop.

   If the local IP Host has the proper route entry to the remote network, refer to *Verify IP Routing Over a LAN Connection* in the *System Verification* chapter.

   If the local IP Host does not have the proper route entry, make corrections to the local IP Host configuration.

IP Routing Over a WAN RLAN Interface Connection

Problem:
The remote IP Host connected to a WAN RLAN interface on the SmartSwitch Remote Access Module does not receive a ping response from the SmartSwitch Remote Access Module WAN RLAN interface.

Action:
1. Verify that the WAN connection is up. Use the *mc* console command to display the Monitor Connections screen. Check for the connection. If the connection is up, then continue with the next step.

   If the connection is not up, refer to *Remote Device Connectivity*.

2. Verify that the WAN RLAN interface is properly initialized. Use SFVRA-CFG to check for the proper WAN RLAN interface (refer to page 77 for instructions). If the proper WAN RLAN interface exists, then continue with the next step.

   If the proper interface does not exist, use SFVRA-CFG to make the necessary corrections.

3. Check that the IP address configured for the IP Host device matches the address configured on the IP Host device. Make corrections to the SmartSwitch Remote Access Module's configuration (using SFVRA-CFG), or to the IP Host's configuration, as required. To do this, follow the instructions outlined on page 84.

Problem:
The remote IP Host connected to a WAN RLAN interface on the SmartSwitch Remote Access Module does not receive a ping response from the SmartSwitch Remote Access Module LAN interface.

Action:
1. Verify that the remote IP Host can access the WAN RLAN interface of the SmartSwitch Remote Access Module. If this can be done successfully, continue with the next step.

   If the remote IP Host is not able to access the WAN RLAN interface, then refer to the preceding problem and action.

2. Verify that the LAN interface is properly initialized. Use SFVRA-CFG (refer to page 77 for instructions) to check for the proper LAN interfaceIf the proper interface exists, then continue with the next step.

   If the proper interface does not exist, use SFVRA-CFG to make the necessary corrections.

3. Verify that the remote bridge device is initiating a call to the SmartSwitch Remote Access Module. Since the SmartSwitch Remote Access Module LAN interface has an IP address assigned with a different network number than the one for the remote IP Host, the remote IP Host may need a proper route entry for the local network where the SmartSwitch Remote Access Module is located. Make corrections to the remote IP Host configuration.

Problem:
The remote IP Host connected to a WAN RLAN interface on the SmartSwitch Remote Access Module does not receive a ping response from the local IP Host.

Action:
1. Verify that the remote IP Host can access the LAN interface of the SmartSwitch Remote Access Module. If it accesses the LAN interface, then continue with the next step.

   If the remote Host is unable to access the LAN interface, refer to the preceding problem and action.

2. Verify that the local IP Host has the route entry for the remote network with the SmartSwitch Remote Access Module as the next hop. If it does, refer to *Verify IP Routing Over a LAN Connection* in the *System Verification* chapter.

   If the local IP Host does not have the proper route entry, make corrections to the local IP Host configuration.

IP ROUTING OVER A WAN UNNUMBERED INTERFACE CONNECTION

Problem:
The remote router connected to a WAN UnNumbered interface on the SmartSwitch Remote Access Module does not receive a ping response from the SmartSwitch Remote Access Module LAN interface.

Action:
1. Have the remote router ping itself using its LAN IP address.

2. Have the SmartSwitch Remote Access Module ping itself using its LAN IP address.

3. Have the router ping the SmartSwitch Remote Access Module. If the ping is unsuccessful:
   - and no call is up, check the static route on the router
   - and a call is up, check the static route on the SmartSwitch Remote Access Module (refer to page 82 for instructions regarding getting to the IP static route information using SFVRA-CFG).

IP RIP

This section provides guidance for diagnosing IP RIP operational problems.

IP RIP INITIALIZATION

Problem:
The SmartSwitch Remote Access Module does not display the correct IP RIP Initialization messages. Instead, it displays one or more of the following message:

```
[IP RIP] Initialization failed, unable to allocate buffers
[IP RIP] Unable to open RIP/UDP port 512
```

Action:
There is an unexpected condition present within the SmartSwitch Remote Access Module software. Contact Customer Support.

IP RIP OUTPUT PROCESSING ON A LAN INTERFACE

Problem:
The local IP Host does not display the correct route entry, for example, the IP Host does not seem to be learning route information from the SmartSwitch Remote Access Module via RIP.

Action:

1. Using SFVRA-CFG, verify that the IP RIP Send Control is set to a RIP version that the IP Host can understand. To check the system's IP RIP Send Control value
   a. If it is not already running, start up SFVRA-CFG.
   b. From the toolbar, select *Functions*, then *IP Network*, then *Systems*, or click on the icon.
   c. Select the system's site from displayed list (you should have already configured IP subnet and network interface information for this site).
   d. Click on the *Network Interface* tab.
   e. Select the appropriate interface.
   f. Click on the *Expert Options* tab.
   g. Check to see that the value selected for RIP Send Control is set to the version the IP Host can understand. If necessary, change the value.
   h. If you made any changes to the configuration, download the updated configuration files to the effected site.

   For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

   - For network interfaces: refer to *Configuring IP Network System Interfaces* in the *Configuring IP Network Information* chapter.

- For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

2. Enter the *`ip rip stats`* administrative console command. Look for the `IfStatSentResponses` counter for the interface, which shows the number of RIP update messages sent on the interface.

   If the counter is 0, enter the *`ip rip send`* administrative console command to force the RIP update message to be sent immediately.

3. Repeat step 2.

   If the counter is still 0, there is an unexpected condition present within the SmartSwitch Remote Access Module software. Contact Customer Support.

4. If the RIP Send Control is set to "RIP Version 1" or "RIP Version 1 Compatibility," verify that the transmit broadcast address on the interface is set to a proper address that the IP Host can receive.

   Change the value using SFVRA-CFG if the transmit broadcast address is not set properly. To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions*, then *IP Network*, then *Systems*, or click on the icon.

   c. Select the system's site from displayed list (you should have already configured IP subnet and network interface information for this site).

   d. Click on the *Network Interface* tab.

   e. Select the appropriate interface.

   f. The *Transmit Broadcast Address* value is under *Properties*. Enter a correction if necessary.

   g. If you made a change, download the updated configuration files to the effected system.

   For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

   - For network interfaces: refer to *Configuring IP Network System Interfaces* in the *Configuring IP Network Information* chapter.

   - For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

5. Check the IP Host and ensure that it is set up to learn route information via RIP.

IP RIP INPUT PROCESSING ON A LAN INTERFACE

Problem:
The SmartSwitch Remote Access Module does not display the correct route entry, for example, the module does not seem to be learning route information via RIP.

Action:
1. Verify that the IP RIP Receive Control is set to the proper RIP version that the Router is using. Refer to page 88 for instructions regarding check RIP versions.

2. Enter the `ip rip stats` administrative console command. Look for the counter `IfStatRcvResponses` for the interface, which show the number of RIP update messages received on the interface.

   If the total number of these counters is 0, check the Router to verify that it is configured to send IP RIP update messages.

3. Also look for the `IfStatRcvBadPackets` and `IfStatRcvBadRoutes` counters.

   If these counters are not 0, there may be something wrong with the Router.

   If these counters are 0, there is an unexpected condition present within the SmartSwitch Remote Access Module software. Contact Customer Support.

IP RIP OUTPUT PROCESSING ON A WAN INTERFACE

Problem:
The Router does not display the correct route entry, i.e., the Router does not seem to be learning route information from the SmartSwitch Remote Access Module system via RIP.

Action:
1. Verify that the IP RIP Send Control is set to the proper RIP version that the Router can understand. Refer to page 88 for instructions regarding check RIP versions.

2. Enter the `ip rip interface` administrative console command. Look for the ***Broadcast Address*** value. This is the IP address of the router that the RIP messages are sent to.

   If the address is not the correct address for the Router, correct the transmit broadcast address for the interface using SFVRA-CFG. Refer to page 89 for instructions regarding checking the address.

3. Enter the `ip rip stats` administrative console command. Look for the ***IfStatSentResponses*** counter for the interface, which shows the number of RIP update messages sent on the interface.

   If the counter is 0, enter the `ip rip send` administrative console command to force the RIP update message to be sent immediately.

4. Repeat step 3).

   If the counter is still 0, there is an unexpected condition present within the SmartSwitch Remote Access Module software. Contact Customer Support.

5. Check the Router and ensure that it is set up to learn route information via RIP.

IP RIP INPUT PROCESSING ON A WAN INTERFACE

Problem:
The SmartSwitch Remote Access Module system does not display the correct route entry, i.e., the system does not seem to be learning route information via RIP.

Action:
1. Verify that the IP RIP Receive Control is set to the proper RIP version that the Router is using. Refer to page 88 for instructions regarding check RIP versions.

2. Enter the `ip rip stats` administration console command. Look for the ***IfStatRcvResponses*** counter for the interface. This statistics is the number of RIP update messages received on the interface.

   If the total number of these counters is 0, check the Router to verify that it is configured to send IP RIP update messages.

3. Also look for the *IfStatRcvBadPackets* and *IfStatRcvBadRoutes* counters.

   If these counters are not 0, there may be something wrong with the Router.

   If these counters are 0, there is an unexpected condition present within the SmartSwitch Remote Access Module system software. Contact customer support.

IPX ROUTING

This section provides methods for diagnosing problems in the following areas of IPX routing:
- IPX routing initialization
- IPX routing over the LAN connection
- IPX routing over the RLAN connection
- IPX routing over the WAN connection
- triggered RIP/SAP start up
- triggered RIP/SAP operation

IPX ROUTING INITIALIZATION

Problem:
The SmartSwitch Remote Access Module does not display the correct IPX Initialization messages. Instead, it displays the following message (display messages by entering the `dr` console command):

```
[IPX] Initialization failure
```

Action:
An internal error has occurred. Contact Customer Support

IPX ROUTING OVER THE LAN CONNECTION

Problem:
The SmartSwitch Remote Access Module does not display the correct message after issuing the *ipx diag* or *ipx ping* command. Instead, it displays the following message:

```
No response from <ipx-address>
```

Action:

1. Verify that the routing entry for the destination network exists by entering the following console command:

   ```
   ipx route
   ```

   If the SmartSwitch Remote Access Module displays the route to the destination, it knows how to reach the local server's internal network. Determine if this is a static route or a dynamic route learned via RIP. The output of an *ipx route* command contains a protocol (P) field for each route entry, which indicate if it is static (L- locally configured) or dynamically learned via RIP (R). If it is learned via RIP, then basic communication between the SmartSwitch Remote Access Module and the local NetWare server is operational, and it is uncertain why the NetWare server does not respond to the ping request. Contact Customer Support.

2. Using SFVRA-CFG, verify that IPX RIP send and receive control is enabled for the LAN interface. To check the system's IPX RIP send and receive control values:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions*, then *IPX Network*, then *Systems*, or click the icon.

   c. Select the system from displayed list.

   d. Click on the *Network Interface* tab.

   e. Select the appropriate interface.

   f. Click on the *Expert Options* tab.

   g. Check to see that RIP send control is set to *send* and RIP receive control is set to *receive*. If they are not, change the values.

   h. If you made any changes to the configuration, download the updated configuration files to the effected site.

   For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

   - For network interfaces: refer to *Configuring IPX Network System Interfaces* in the *Configuring IPX Network Information* chapter.

   - For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

3. If the route does not exist, or the route is a static entry, then verify that the SmartSwitch Remote Access Module and the local NetWare server are using the same packet encapsulation. To check the type of encapsulation, use SFVRA-CFG. The packet encapsulation type is configured

on the same *Expert Options* screen described in the above action. If they are not using the same encapsulation, then correct it either on the SmartSwitch Remote Access Module or the NetWare server.

4. Verify that the SmartSwitch Remote Access Module and the NetWare server are using the same external IPX network number for their mutual LAN (AA for this example). To check the network number that the SmartSwitch Remote Access Module is using, use SFVRA-CFG. If they are not using the same external network number, then correct the problem. To check or change the SmartSwitch Remote Access Module's external network number:

   a. It it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions*, then *IPX Network*, then *Systems*, or click the icon.

   c. Select the IPX segment in question from displayed list.

   d. Under the Properties tab, check the segment's External Network Number. Make a change if necessary.

   e. If you made any changes to the configuration, download the updated configuration files to the effected site.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For network interfaces: refer to *Configuring IPX Network System Interfaces* in the *Configuring IPX Network Information* chapter.
- For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

IPX ROUTING OVER THE REMOTE LAN CONNECTION

Problem:
The system does not display the IPX messages indicating successful initiation on Remote LAN network.

Action:
Using SFVRA-CFG, check the IPX network interface configuration. To do this:

1. It it is not already running, start up SFVRA-CFG.
2. From the toolbar, select *Functions*, then *IPX Network*, then *Systems*, or click the icon.
3. Select the system from displayed list.
4. Click on the *Network Interfaces* tab.
5. Select the appropriate interface and check the interface configuration for possible errors. Make corrections as needed.

6. If you made any changes to the configuration, download the updated configuration files to the effected site.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For network interfaces: refer to *Configuring IPX Network System Interfaces* in the *Configuring IPX Network Information* chapter.
- For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

Problem:
Data is not forwarded from the remote bridge to the router over the Remote LAN interface.

Action:
Check the configuration:
1. Verify Remote LAN interface configuration. Refer to the above action for instructions regarding checking an interface's configuration.

2. Verify device configuration on remote bridge. Bridge devices should be configured to make calls over the interface defined to go to the router.

Problem:
The router does not forward typical data (RIP, SAP, Type 20 packets) to the remote bridge.

Action:
1. Make sure a call is up. Remember, the router cannot forward data if there is no previous connection (i.e., router currently does not support dial-out).

2. Check IPX device information on the router side. Instructions for accessing the device's IPX information are on page 93.

Problem:
Data is not received by a remote client (or server) on a Remote LAN network, but the call does come up between the router and the remote bridge.

Action:
1. Double check and resolve any configuration / connection problems for the client (or server) to the bridge on the Remote LAN. (Basically, eliminate the possibility of any LAN configuration problems which are unrelated to the Remote LAN interface).

2. If you determine the problem is related to the Remote LAN, verify the IPX Network Number for the remote bridge in the router's configuration (under bridging properties). Refer to page 93 for instructions on checking the IPX Network Number.

IPX ROUTING OVER THE WAN CONNECTION

Problem:
The remote NetWare server does not appear in the NetWare client's network neighborhood.

Action:
1. Verify that the SmartSwitch Remote Access Module has SAP process enabled. To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions*, then *IPX Network*, then *Systems*, or click on the icon.

   c. Select the system's site from displayed list (you should have already configured IPX segment information for this site).

   d. Click on the *Network Interface* tab.

   e. Select the appropriate interface.

   f. Click on the *Expert Options* tab.

   g. Check to see that the *SAP Configuration* value is set to *Send.*

   h. If you made any changes to the configuration, download the updated configuration files to the effected site.

   For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

   - For network interfaces: refer to *Configuring IPX Network System Interfaces* in the *Configuring IPX Network Information* chapter.
   - For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

TRIGGERED RIP/SAP START UP

Problem:
The SmartSwitch Remote Access Module does not display a triggered RIP/SAP starting message for a WAN peer.

Action:
Verify that the WAN peer is properly configured. Be sure that the device (WAN peer) has IPX routing enabled and triggered RIP/SAP (active) selected as routing protocol.

TRIGGERED RIP/SAP OPERATION

Problem:
Routes or Services are not propagated between peers.
Changes are not propagated between peers.

Action:

1. Verify triggered RIP / SAP has successfully started for peers. Issue the `dr` console command and look for the "starting" message in the log.

2. Generate a triggered RIP / SAP update request to the devices in question. Issue the following console command for each device:
   ```
   ipx trigreq <device>
   ```

3. Verify that the statistics are incremented properly. Issue the following console commands:
   ```
   ipx trigrip stats
   ipx trigsap stats
   ```

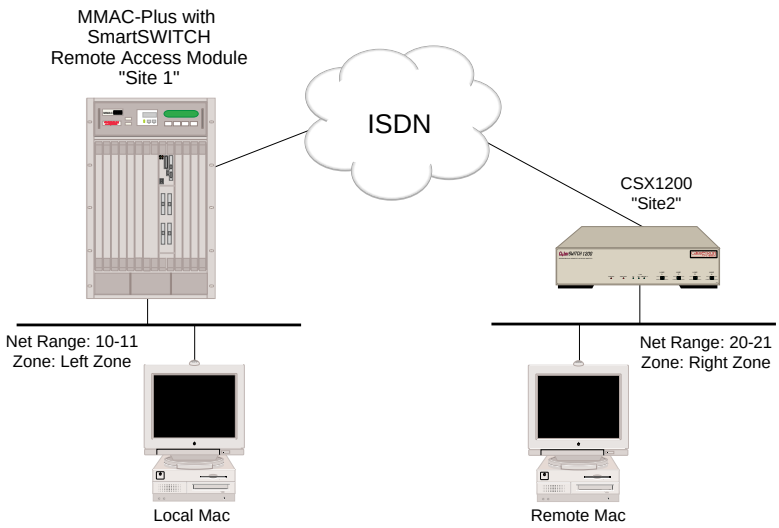
4. If routes / services are not propagated on either side, contact Customer Support.

APPLETALK ROUTING

This section provides methods for diagnosing problems in the following areas of AppleTalk routing:

- AppleTalk routing initialization
- AppleTalk routing over the LAN connection
- AppleTalk routing over the WAN connection

Use the following example configuration to diagnose AppleTalk routing operational problems. The example below uses AppleTalk addresses, zones, and resource names specific to the example. Substitute those of your network when you perform the diagnosis steps.



APPLETALK ROUTING INITIALIZATION

Problem:

The SmartSwitch Remote Access Module does not display the correct AppleTalk Routing Initialization messages.

Action:

1. Using SFVRA-CFG, check the system configuration. Make sure that the AppleTalk feature is enabled for the system. To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions* then select *Sites* or click the icon.

   c. From the displayed list, double click on the site in question.

   d. Click on the *Systems* tab.

   e. Select the system in question, then click on *Edit System Settings.*

   f. Under *AppleTalk* information, check to make sure that a check appears next to *Enable* (AppleTalk information is included under the *Properties* tab).

   g. If you made a change, download the new configuration files to effected site.

   For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

   - For enabling AppleTalk: refer to *Configuring the Site's Systems* in the *Configuring Sites* chapter.
   - For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

APPLETALK ROUTING OPERATIONAL OVER THE LAN CONNECTION

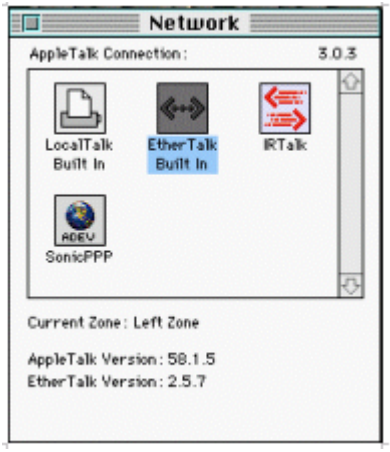
Problem:
No zones appear in the Mac's Chooser.

Action:

1. Verify that the AppleTalk LAN port that Local Mac is attached to is in *up state* by entering the following console command:
   ```
   atalk port
   ```
   If the command shows the port is not in up state, wait for a couple of minutes and repeat this step.

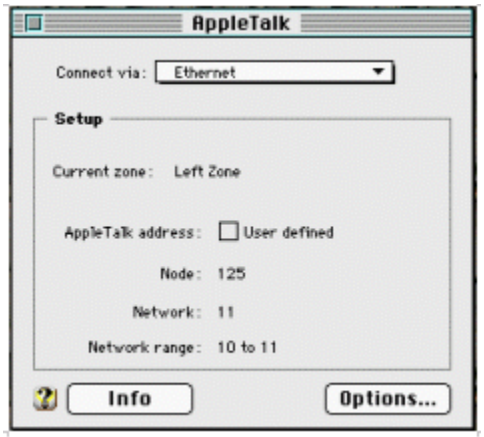
2. Check to see if the LAN connection of the port is operational. If the LAN connection is not operational, then correct the problem.

3. If you are using Classic Networking, verify that EtherTalk is used on the Local Mac by opening the Network control panel as shown below:



If EtherTalk is selected, and no zones are displayed, then contact your Distributor or Customer Support.

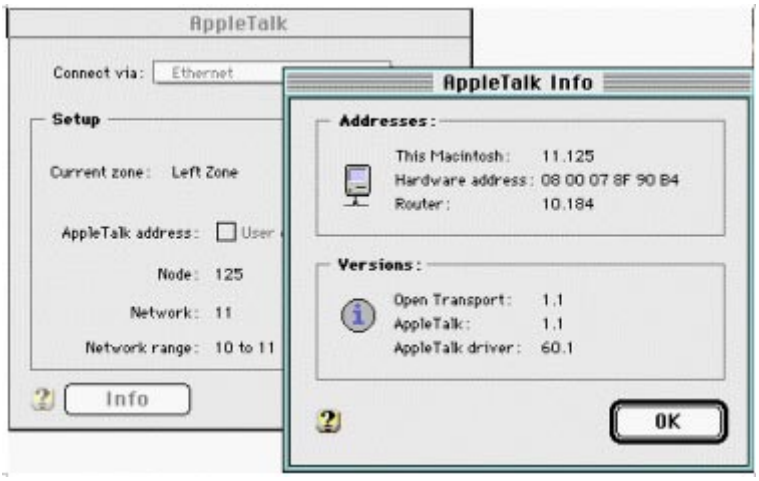
4. If you are using Open Transport, verify that Local Mac has chosen a proper AppleTalk address within the valid network range (this would be 10-11 for the example network) by opening the AppleTalk control panel as shown below:



If the Network Range is correct and the AppleTalk address is not within that range, then try to close the AppleTalk control panel once, and then reopen it. If the AppleTalk address is still invalid, then try to assign a valid address manually by marking *User defined* box. If you start seeing zones, then you can take out the *User defined* tag.

If the Network Range is not correct, contact your Distributor or Customer Support.

5. If the AppleTalk address of Local Mac is valid, then check which AppleTalk router that Local Mac is obtaining the information from by selecting *info* box in the AppleTalk control panel as shown below (this can be done if *Open Transport* is being used):



If the AppleTalk address for the router is not same as the one displayed when issuing `atalk port` console command, then the Local Mac is getting the information from another router. Please refer to the document for the router.

If the AppleTalk address for Router is the same as the one displayed after issuing the `atalk port` console command, contact your Distributor or Customer Support.

Problem:
Only local zones appear and remote zones are not shown in the Mac's Chooser:

Action:
1. Verify that a static route to the remote network is properly configured on the SmartSwitch Remote Access Module. The static route is configured using SFVRA-CFG.

2. If the static route is not configured correctly, make the appropriate corrections. To check the AppleTalk static routing information:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions*, click *AppleTalk Network,* then *Systems*, or click on the toolbar.

   c. Double click on the system in question.

   d. Click on the *Static Routes* tab.

   e. Double click on the static route in question.

   f. Verify the information entered for the static route. Make any necessary changes.

   g. If you made any changes, download the new configuration files to the site.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For AppleTalk static route information: refer to *Configuring AppleTalk Network System Static Routes* in the *Configuring AppleTalk Network Information* chapter.
- For downloading updated configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

3. If the static route is properly configured, then contact your Distributor or Customer Support.

APPLETALK ROUTING OPERATIONAL OVER THE WAN CONNECTION

Problem:
The local Mac is unable to see the remote resource (Remote Mac), which is located across the WAN.

Action:
1. Verify that AppleTalk Routing is operational on both the local and the remote LAN.

2. Verify that the remote resources (remote Mac) can be seen when the WAN connection is up.

3. If the remote resources can be seen when the connection is up but not when the connection is down, there are some problems with making outbound calls. Using SFVRA-CFG, make sure that the information on the remote SmartSwitch Remote Access Module (labeled *Site 2* in the example network) contains a proper AppleTalk address, and that *Make calls for AppleTalk data* for the device is *enabled.*

   To check the system's AppleTalk address and ensure that *Make calls for AppleTalk data* is enabled:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions* then select *Connection Groups* or click the icon.

   c. Click on the site's connection group (this should have been configured previously).

   d. Click on the site in question, then on the same screen, click on *Edit Group Connections.*

   e. Double click on the connection in question.

   f. Click on the *Protocols* tab.

   g. Click on the *AppleTalk* tab.

   h. On this screen, make sure AppleTalk is enabled for the connection, and make sure *Make calls for AppleTalk data* is enabled for the site(s) that needs to be able to initiate AppleTalk calls.

   i. On the same screen, make sure that the correct AppleTalk segment has been selected for this segment. Choices include: none, unnumbered, and the AppleTalk segments you have configured. The value selected should be either unnumbered or one of the configured AppleTalk segments. If the value selected is a configured AppleTalk segment, you will

need to examine the segment's configuration to check the actual AppleTalk address (using steps *i* through *m* below). If the value selected is *unnumbered*, continue with step *n*.

j. From the toolbar, select *Functions*, click *AppleTalk Network*, then *Systems*, or click on the toolbar.

k. Double click on the system in question.

l. Click on the *Ports* tab.

m. Double click on the WAN segment identified in step *i* above.

n. Verify the information entered for the *Network Number* and *Node ID*. These values make up the AppleTalk address. Make any necessary changes.

o. If you made any changes, download the new configuration files to the site.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For AppleTalk configuration group information: refer to *Adjusting Protocol Information* in the *Configuring Connection Groups* chapter.
- For AppleTalk address information: refer to *Configuring AppleTalk Network System Ports* in the *Configuring AppleTalk Network Information* chapter.
- For downloading updated configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

4. If the remote resources can not be seen even when the connection is up, then make sure the AppleTalk address of the remote device is valid. If the remote device is on an unnumbered network, then AppleTalk an address of 0.0 must be configured for the remote device. If it is on a numbered network, the AppleTalk address does not need to be configured for the device. However, if it is configured, it must match the AppleTalk address configured on the remote device.

SNMP

Problem:
The SNMP Agent is not functioning.

Action:
1. Using SFVRA-CFG, check the configuration of the SmartSwitch Remote Access Module. In order for the SNMP Agent to become enabled, both the IP option and the SNMP Agent must be enabled in the SmartSwitch Remote Access Module configuration. The site must be configured in an *SNMP Management Group*.

   a. If it is not already running, start up SFVRA-CFG.

   b. To see if IP is enabled for the system:

   - From the toolbar, select *Functions* then select *Sites* or click the icon.

- From the displayed list, double click on the site you are diagnosing.
- Click on the *Systems* tab.
- Select the system, then click on *Edit System Settings*.
- Under IP information (on the *Properties* screen), check to make sure that a check appears next to *Enable*.
- If you made a change, download the new configuration files to effected site.

c. To see if SNMP is enabled for the system:

- From the toolbar, select *Functions* then select *SNMP* or click the

icon.
- Double click on the SNMP Management Group that the site is associated with.
- Click on the *Managed Sites* tab.
- Check to see if the site in question is included in the managed sites list. If not, click on *Add*, and enter the information to add the site to the group.
- Once you add the site, or if it is already included in the group, check to see that *Enabled* appears in the site's *SNMP* column. Note that SNMP is enabled at the site template level. If SNMP is not enabled for this site, you must select a site template for the site that has SNMP enabled. To select a different site template for the site:

  From the toolbar, select *Functions* then select *Sites* or click the icon.

  Double click on the site in question.

  Select a new site template for the site – one that has SNMP enabled. If you do not have a template configured with SNMP enabled, you will have to create one. If all or most the other values of an existing template are acceptable, you may duplicate that template, give it a different name, and make changes where necessary.

d. If you made any changes, download the new configuration files to the site.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For enabling IP: refer to *Configuring the Site's Systems* in the *Configuring Sites* chapter.
- For SNMP Management Group information: refer to the *Configuring SNMP Management Groups* chapter.
- For information about choosing a site's template: refer to *Configuring Site Properties* in the *Configuring Sites* chapter.
- For information about duplicating a site's template: refer to *Adding a Site Template* in the *Configuring Site Templates* chapter.

- For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

2. Enter the *dr* command at the administrative console. If the following message appears, the IP subsystem has initialized successfully:
   ```
   [IP] IP router is initialized successfully
   ```

3. However, if one of the following messages appears, there is an unexpected condition present within the SmartSwitch Remote Access Module software. Contact Customer Support.
   ```
   [SNMP] SNMP initialization failure - unable to allocate necessary
          memory
   [SNMP] SNMP initialization failure - unable to open UDP port
   ```

Problem:
The SmartSwitch Remote Access Module does not respond to SNMP requests.

Action:
1. Enter the command *snmp stats* at the administrative console. If an "`SNMP is not enabled`" message appears, you must first enable the SNMP Agent. For detailed instructions for enabling the SNMP agent, refer to page 102.

2. If the SNMP statistics are displayed, check the value of the "snmpInBadVersions" statistic. If it is non-zero, the Network Management station is generating request PDUs with an incompatible SNMP version number. Such requests are discarded by the SNMP agent.

3. Check the value of the "snmpInBadCommunityUses" statistic. If it is non-zero, the community name specified in the request PDUs does not have the proper access rights to perform the desired request, and the request is discarded. To correct this problem, reconfigure the MIB access level for the desired community name to the desired access level.

4. Check the value of the "snmpInASNParseErrs" statistic. If it is non-zero, the network management station is generating request PDUs that are not properly encoded in ASN.1 format. Such requests are discarded by the SNMP agent.

Problem:
The SmartSwitch Remote Access Module does not generate SNMP Trap PDUs.

Action:
1. Enter the *snmp stats* command at the administrative console. If an "SNMP is not enabled" message appears, you must first enable the SNMP Agent. For detailed instructions for enabling the SNMP agent, refer to page 102.

2. If the SNMP statistics are displayed, check the value of the "`snmpOutTraps`" statistic. If this counter is zero, the SNMP agent has not generated any Traps. Check your configuration setup and ensure that at least one SNMP Trap Receiver is configured. If the value of the "`snmpOutTraps`" statistic is non-zero, the SNMP agent is generating Trap PDUs. If a given Network Management Station is not receiving Traps as expected, check your configuration setup and ensure that the IP address and the Community Name of the Network Management Station that is not receiving Traps is configured properly.

3. Enter *dr* at the administrative console to display the current system messages. If one of the following messages appears, the SNMP agent does not have enough memory to generate all of the Trap PDUs that need to be generated. If the "snmpOutTraps" counter is not increasing while these reports are being logged, there is an unexpected condition present within the SmartSwitch Remote Access Module System software. Contact Customer Support.

```
[SNMP] Unable to obtain an SNMP Trap queue header
[SNMP] Unable to obtain an SNMP Trap queue entry buffer
```

Problem:
The following message is continuously reported in the system log (enter the *dr* console command to display the system log):

```
[SNMP] Authentication failure, unknown community name
```

Action:
The Community Name specified in the request PDUs is not recognized by the SNMP Agent. To correct this problem, use SFVRA-CFG to add the desired community name or change the configuration of your Network Management Station so that it uses a Community Name that is known to the SmartSwitch Remote Access Module.

To add the desired community name to the site:

1. If it is not already running, start up SFVRA-CFG.
2. From the toolbar, select *Functions* then select *SNMP* or click the

icon.
3. Double click on the SNMP Management Group that the site is associated with.
4. Click on the *Communities* tab, then click on *Add*.
5. Enter a *Community Name*, then select an associated *MIB Access Level*, then click on *Add*.
6. If you made any changes, download the new configuration files to the site.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For SNMP community name information: refer to *Configuring SNMP Management Group Communities* in the *Configuring SNMP Management Groups* chapter.
- For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

Problem:
The following message is continuously reported in the system log (display the system log by issuing the *dr* console command):

```
[SNMP] Authentication failure, improper access rights
```

Action:
The Community Name specified in the request PDUs does not have the proper access rights to perform the desired request. Use SFVRA-CFG to change the MIB access level of the indicated Community Name to the desired access level or change the configuration of your Network Management Station so that it uses a Community Name that has the desired MIB access level.

To change a MIB access level:

1. If it is not already running, start up SFVRA-CFG.
2. From the toolbar, select *Functions* then select *SNMP* or click the

icon.
3. Double click on the SNMP Management Group that the site is associated with.
4. Click on the *Communities* tab.
5. Since you cannot edit the MIB access level for a previously configured Community Name, you will need to delete the Community Name, and then add it back with a corrected access level. To do this:
    a. Select the Community Name in question, then click on *Delete*.
    b. Click on *Add*, then enter the new *Community Name* and the corrected associated *MIB Access Level*. Click on *Add*.
6. If you made any changes, download the new configuration files to the site.

For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

- For SNMP MIB access level information: refer to *Configuring SNMP Management Group Communities* in the *Configuring SNMP Management Groups* chapter.
- For downloading configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

DIAL OUT

Problem:
A Dial Out call was not completed successfully.

Action:
1. If you issued the `call device <device name>` console command to initiate the call, check to see that you entered the device name correctly. Device names are case sensitive.
2. If you issued the `call peer <telephone number data rate>` console command to initiate the call, check to see that you entered the correct telephone number and data rate. The telephone number must contain all required prefixes such as the area code, or a "9" if Centrex is used.

3. If you have entered the call device or the call peer command correctly, follow the set up and actions listed below.

Set Up:

1. Enable the call trace messages by issuing the *trace on* console command.

2. Erase the current system messages (issue the *er* console command).

3. Initiate a call to a remote device by issuing the *call device <device name>* console command.

4. Display the system messages (issue the *dr* console command).

5. Look for the following call request messages among the system messages.

```
Out - CALL RQST ACK Call Id=<call Id> Rate=<data rate> Slot=<slot#>
   Port=<port#> Chans=<bearer channel map> TN=<telephone number di-
   aled> Ces=<communication endpoint suffix> ConnId=<connect Id
In - CALL RQST ACK CallId=<call Id> Slot=<slot#> Port=<port#>
   CES=<ces> ConnId=<connection Id>
In - PROCEEDING Call Id=<call Id> Slot=<slot #> Port=<port #>
   Chans=<bearer channel map> Ces=<communication endpoint suffix>
   ConnId=< connect Id>
In - CONNECT Call Id=<call Id> Slot=<slot#> Port=<port #>
   Chans=<bearer channel map> Ces=<communication endpoint suffix>
   ConnId=<connect Id>
```

Action:

1. If the system does not report a call request message for the remote device, then the system did not attempt to make a call. Check to see if there is enough call resources (lines, channels, supported connections) to make the missing call. For example, if your system supports only one BRI line, and you have no hunt groups, then only two active connections are possible. The system would not attempt to make a third call.

   If this is not the case, contact Customer Support.

2. If the system reports a call request message but it does not connect, then the system attempted to make a call. Check to see if the remote device has already completed the installation and verification processes, and is currently running with no active errors.

   If there are no problems with actions 1 and 2, proceed to action 3.

3. Check for the following system messages:

```
In - accept <#,#>
In - disconnect <#,#> - <disconnect cause>
```

   If the system reports these messages, then the network disconnected the call attempt. For the disconnect cause meaning, refer to the *Cause Code* table. If help is necessary to resolve the reported disconnect cause, write down the "disconnect cause" and call your phone company (carrier) to report the problem.

COMPRESSION

Problem:

Compression is not established for a device for which it is expected.

Action:

1. Issue the `cmp stats` console command then issue the `dr` console command to check the message report log. A message will inform you if the compression failed due to memory constraints.

2. Use SFVRA-CFG to verify that the SmartSwitch Remote Access Module has compression enabled. To do this:

   a. If it is not already running, start up SFVRA-CFG.

   b. From the toolbar, select *Functions* then select *Connection Groups* or click the icon.

   c. Click on the site's connection group (this should have been configured previously).

   d. Click on the site in question, then on the same screen, click on *Edit Group Connections.*

   e. Double click on the connection in question.

   f. Click on the *Access* tab.

   g. If it is not enabled, enable *Compression* for this connection.

   h. If you made any changes, download the new configuration files to the site.

   For more detailed instructions, refer to the following sections in the *SFVRA Configuration Manager User's Guide:*

   - For compression information: refer to *Adjusting Access Information* in the *Configuring Connection Groups* chapter.

   - For downloading updated configuration files: refer to *Downloading Configuration Updates* in the *Exporting Configuration Files* chapter.

3. Verify that the device to which the connection is being established has compression enabled. If the device is another SmartSwitch Remote Access Module, refer to the previous step for instructions.

4. Use the trace console command to examine the CCP frames exchanged with the device. This is typically accomplished by issuing the `trace ppp on` command, erasing the log contents, establishing the call, and then examining the log again (by issuing the `dr` console command) to view the frame trace.

   The following traces illustrate some common PPP startup scenarios when compression is enabled. Only the CCP frames are excerpted for clarity.

   - *Successful Negotiation*
     As a reference, the following trace illustrates a successful negotiation of CCP using the Stac

compression protocol. The key feature of this sequence is that each side receives a CONFIG-ACK to its respective CONFIG-REQ.

```
(I) 15:35:09.98 #80FD: Conn=001 OUT-PPP:CCP      CFG REQ Id=0xB4 Len=9
(I) 15:35:09.98 #9999: -Alg: 0x11 (STAC-LZS) Len: 5
(I) 15:35:09.98 #9999:   Hist Count: 01   Chk Mode: 0x03 (SEQ#)
(I) 15:35:09.98 #80FD: Conn=001 IN -PPP:CCP      CFG REQ Id=0x7B Len=9
(I) 15:35:09.98 #9999: -Alg: 0x11 (STAC-LZS) Len: 5
(I) 15:35:09.98 #9999:   Hist Count: 01   Chk Mode: 0x03 (SEQ#)
(I) 15:35:09.99 #80FD: Conn=001 OUT-PPP:CCP      CFG ACK Id=0x7B Len=9
(I) 15:35:09.99 #9999: -Alg: 0x11 (STAC-LZS) Len: 5
(I) 15:35:09.99 #9999:   Hist Count: 01   Chk Mode: 0x03 (SEQ#)
(I) 15:35:09.99 #80FD: Conn=001 IN -PPP:CCP      CFG ACK Id=0xB4 Len=9
(I) 15:35:09.99 #9999: -Alg: 0x11 (STAC-LZS) Len: 5
(I) 15:35:09.99 #9999:   Hist Count: 01   Chk Mode: 0x03 (SEQ#)
```

- *Peer Protocol-Rejects CCP*
  If the peer does not actually support PPP compression, it will most likely Protocol-Reject the SmartSwitch Remote Access Module's attempt to negotiate CCP. In this case, the SmartSwitch Remote Access Module will abandon its attempt to use compression and the connection will operate uncompressed. The incoming frame from the peer contains a PROT-REJ, whose 1st two hex octets in the trace indicate the CCP protocol (0x80FD).

```
(I) 16:01:51.65 #80FD: Conn=001 OUT-PPP:CCP      CFG REQ Id=0x87 Len=9
(I) 16:01:51.65 #9999: -Alg: 0x11 (STAC-LZS) Len: 5
(I) 16:01:51.65 #9999:   Hist Count: 01   Chk Mode: 0x03 (SEQ#)
(I) 16:01:51.65 #C021: Conn=001 IN -PPP:LCP      PROT REJ Id=0x00 Len=15
(I) 16:01:51.71 #0000:   80 FD 01 87 00 09 11 05 00 01 03
```

- *The SmartSwitch Remote Access Module does not have Compression ENABLED*
  In this case, the SmartSwitch Remote Access Module will respond to all attempts by the peer to open CCP with a TERM-ACK frame. The connection will operate uncompressed. (Note: a device that supports compression but has it disabled will typically do the exact same thing).

```
(I) 15:36:40.54 #80FD: Conn=001 IN -PPP:CCP      CFG REQ Id=0xEC Len=9
(I) 15:36:40.54 #9999: -Alg: 0x11 (STAC-LZS) Len: 5
(I) 15:36:40.54 #9999:   Hist Count: 01   Chk Mode: 0x03 (SEQ#)
(I) 15:36:40.54 #80FD: Conn=001 OUT-PPP:CCP      TERM ACK Id=0xEC Len=4
```

SYSTEM MESSAGES

OVERVIEW

System Messages provide useful system information. They are listed in the system's report log, a memory resident table. To manipulate the report log, use the following commands at the administrative console:

dr or *ds*	display reports or display statistics
er or *es*	erase current messages / statistics from memory
wr or *ws*	write reports / statistics to disk

When the SmartSwitch Remote Access Module writes system messages to disk, it stores them in the following locations:

Directory:	`\log`
File Name:	`rprt_log.nn` (where "nn" is an integer from 1 to 10 that is incremented each time a new file is written.)

The system reports messages using the following format:

Message Type		Time	Report Number	Message
I	Informational	hour:minutes:second	internal ID for area reporting the message	actual text of the message
W	Warning			
E	Error			

- the Message Type quickly identifies the type of message the system reports
- the Time identifies when the message was reported
- the Report Number is used by your Distributor or Customer Support
- the Message text describes the actual message being reported

This chapter describes the types of system messages available (for example, informational and error). It also lists each message individually, with suggested actions to take in the event of an error.

Note: Some of the system messages will not appear on all platforms.

There is another chapter that is of major importance when dealing with system messages. The Problem Diagnosis chapter describes the process of diagnosing common problems, (particularly in the system verification process,) as well as providing possible recoveries.

INFORMATIONAL MESSAGES

The system records informational messages. These are normal events that provide you with current system status. Informational messages include the following categories of messages:

- initialization messages
- normal operation messages
- Spanning Tree messages

INITIALIZATION MESSAGES

The system reports a variety of messages during a successful system initialization. These messages may include: status of bridge, status of LAN ports and adapters, data link, SNMP, and TFTP information. The following are examples of typical initialization messages:

```
Bridge is operating in UNRESTRICTED mode
Data link up: Slot=<slot #> Port=<port #> Ces=<comm. endpoint suffix>
[SNMP] SNMP initialized successfully
```

NORMAL OPERATION MESSAGES

The system normal operation messages may include information such as:

```
Call Restrictions have been disabled by user command
WAN Port is now in the <new state> state
```

SPANNING TREE MESSAGES

The Spanning Tree protocol is only supported by the Ethernet-2 interface card.
Spanning Tree protocol messages are prefaced with [STP]. During normal operation, when Spanning Tree protocol is enabled, the system may report informational messages such as:

```
[STP] A new Root Bridge has been detected
[STP] LAN Port <port #> is now a Designated Port
```

WARNING MESSAGES

System warning messages signal events that you should investigate. These messages may be normal during certain network conditions, or they may indicate a problem. The system should continue to operate after posting a warning message. If the system fails to operate normally, then report it using the problem report form included in *Getting Assistance.*

ERROR MESSAGES

When the system detects errors, it reports error messages. If the faulty component cannot be identified, and an error condition persists, then report the error by using the problem report form included in *Getting Assistance*.

SYSTEM MESSAGE SUMMARY

The following pages list all the informational, warning and error messages alphabetically. The text describes the messages, and includes suggestions for problem resolution (if applicable). Note that the trace messages have been isolated for your convenience, and are summarized in the next chapter.

<timestamp> #000: Couldn't open the file C:\SYSTEM\PLATFORM.NEI
The open operation failed, no further detail is available.

<timestamp> #0000: Error reading C:\SYSTEM\PLATFORM.NEI
The read operation failed, perform a software upgrade to reinstall the file.

<timestamp> #0000: Error reading platform type: there is no "plat name" field
There is no <platform name> value following the "=" character in the "current setting" string.

<timestamp> #0000: Error reading platform type: there was no "=" in the string
The "current setting" string has the format "<platform type>=<string>". This error message indicates that no "=" character exists in the string.

<timestamp> #0000: Error reading platform type: type value is too large
The <platform type> value in the "current setting" string is too large to represent an actual platform type.

<timestamp> #0000: Error reading platform type: type was not converted to an int
The <platform type> value in the "current setting" string could not be converted to an actual platform type.

1 port LAN Adapter, operating in remote mode only
This is an initialization message. It identifies the Ethernet adapter type (Ethernet-1), and operating mode. Remote bridging is supported.

2 port LAN Adapter, operating in local and remote mode
This is an initialization message. It identifies the Ethernet adapter type (Ethernet-2), and operating mode. Both local and remote bridging are supported.

aarp found duplicate AppleTalk address <AppleTalk Address> @ <MAC address>
The address resolution protocol found duplicate AppleTalk addresses for this AppleTalk network. Check the configuration for the AppleTalk ports' network range / number.

Abnormal response rcvd: <state msg reason cc state>
An unexpected message was received from a WAN interface card. The <parameters> included are for problem reporting purposes only. If the system fails to operate normally, or the warning continues to occur, contact your Distributor or Customer Support.

A call has exceeded the configured maximum duration
A call has been up longer than the amount of time configured. The next log message will inform the user whether or not the call has been taken down.

ACE authentication is not available. You must first ENABLE ACE user level authentication.
An attempt was made to configure the Terminal Server Security for ACE and ACE was not configured on the SmartSwitch Remote Access Module.

Adapter does not respond: adapter #'x'
The WAN card initialization subsystem encountered an error on the indicated adapter. Restart the system. If the problem persists, the indicated adapter card may be faulty and you should contact your Distributor or Customer Support.

Adapter #'x' failed to initialize
The operational software on the indicated adapter card failed to signal that initialization was completed. Restart the system. If the problem persists, the indicated adapter card may be faulty and you should contact your Distributor or Customer Support.

Adapter #'x' failed to respond from bootstrap
The WAN card initialization subsystem encountered an error on the indicated adapter while downloading the bootstrap program. Restart the system. If the problem persists, the indicated adapter card may be faulty and you should contact your Distributor or Customer Support.

Adapter failed to respond while programming: adapter 'x'
The WAN card initialization subsystem encountered an error on the indicated adapter while programming the hardware. Restart the system. If the problem persists, the indicated adapter card may be faulty and you should contact your Distributor or Customer Support.

Administrative Session using ACE does not support password change.
Passwords may only be changed via the ACE Server administrator initiation. During an administrative login, the user attempted to change password. ACE only supports password change initiated by ACE Server administrator.

AppleTalk routing initialized successfully.
This message is posted when the system AppleTalk routing feature has initialized successfully.

AppleTalk routing RTMP initialization error, AppleTalk disabled
AppleTalk is disabled because there is an initialization problem with the Routing Table Maintenance Protocol (RTMP). Contact your distributor or Customer Support.

AppleTalk routing ZIP initialization error, AppleTalk disabled
AppleTalk is disabled because there is an initialization problem with the Zone Information Protocol (ZIP). Contact your distributor or Customer Support.

AppleTalk successfully initialized on LAN port <port number> with address <AppleTalk address>.
This message is posted when the specified AppleTalk LAN port has initialized successfully.

AppleTalk successfully initialized on WAN port with address <AppleTalk address>.
This message is posted when the specified AppleTalk WAN port has initialized successfully.

Attempting to Autobaud, Press <CR> Many Times, Quickly
The user has requested that the RS 232 port undergo an autobaud procedure, or the RS232 port has not been properly Autobauded.

Attempting to load "<FileName>" for Upgrade
A Reliable Remote Upgrade has taken place. The specified file is now being loaded into memory for verification and subsequent installation into the Flash File System.

Attempt to reinitialize DM card in slot <slot #>
The system is attempting to initialize the Digital Modem card again after a failed attempt. Check the subsequent log messages for the status of the card.

Attempt to initialize unconfigured DM card in slot <slot #>
The system is attempting to initialize a Digital Modem card, with no success. This is likely a configuration problem. Check SFVRA-CFG setup to ensure that it correctly matches existing hardware.

[AUTH] ACE Client has not been initialized.
The ACE client has not been initialized. No service file exists. Server should be expecting SmartSwitch Remote Access Module client to request node verification. Contact the ACE administrator and request the client to be reinitialized.

[AUTH] ACE Could not create service file.
The SmartSwitch Remote Access Module ACE client was in an initialized state. After receiving service information from the ACE server a local file create error occurred while attempting to save the information.

[AUTH] ACE Could not synchronize client-server.
During an authentication attempt the client was unable to synchronize with the server and the user was rejected. The server may not be responding to the client.

[AUTH] ACE Could not write service file.
The SmartSwitch Remote Access Module ACE client was in an initialized state. After receiving service information from the ACE server a local file write error occurred while attempting to save the information.

[AUTH] ACE Decryption of server response failed.
Sever response to an ACE client request was received, but could not be decrypted. Verify encryption method configured for server is accurate.

[AUTH] ACE Encryption configured for DES: not supported.
The ACE server is configured for DES encryption. Only SDI encryption is currently supported by the ACE client.

[AUTH] ACE Error receiving server log message acknowledgment.
A client syntax error occurred during an authentication attempt via ACE. The server did not respond to the logging of the message. Make sure the ACE server configuration is accurate.

[AUTH] ACE LOGIN rejected user: <user name>
The remote Authentication server rejected the named user. This indicates that one of the following has occurred:

1. The <user name> is not in the remote Authentication server's database.

2. The <user name> is entered incorrectly in the remote Authentication server's database.

[AUTH] ACE Node verification received; Client initialized.
The SmartSwitch Remote Access Module ACE client was in an initialized state. Node verification was received from the server and the initialization cycle is complete.

[AUTH] ACE No server configured for designated database location.
ACE is configured as a database location for security authentication. Either no ACE server has been configured or an error occurred when parsing the ACE server configuration.

[AUTH] RADIUS CHAP rejected for device: <device name>
The remote Authentication server rejected the CHAP mode authentication request for the indicated device. This usually indicates that one of the following has occurred:

1. The <device name> is not in the remote Authentication server's database.

2. The device's CHAP response was not calculated properly.

3. The device's SECRET does not match the secret in the RADIUS server's database.

4. The RADIUS server's database entry for this device contains errors.

[AUTH] RADIUS HDLC BRIDGE rejected bridge address: <mac address>
The remote Authentication server rejected the bridge address. This indicates that one of the following has occurred:

1. The <mac address> is not in the remote Authentication server's database.

2. The <mac address> is entered incorrectly in the remote Authentication server's database.

[AUTH] RADIUS INTERFACE LOOKUP rejected name <interface name>
The remote Authentication server route lookup feature rejected the interface name. This indicates that one of the following has occurred:

1. The < interface name> is not in the remote Authentication server's database.

2. The < interface name > is entered incorrectly in the remote Authentication server's database.

[AUTH] RADIUS IP HOST rejected IP Host id: <IP host Id>
The remote Authentication server rejected the IP Host id. This indicates that one of the following has occurred:

1. The <IP Host Id> is not in the remote Authentication server's database.

2. The <IP Host Id> is entered incorrectly in the remote Authentication server's database.

[AUTH] RADIUS IP RESOLVE rejected IP Address: <IP address>
The remote Authentication Server rejected the IP Address Resolution authentication request for the indicated IP Address. This usually indicates that one of the following has occurred:

1. The <IP Address> is not in the remote Authentication server's database.

2. The Authentication server's database entry for this IP Address contains errors.

[AUTH] RADIUS LOGIN rejected device: <device name>
The remote Authentication server rejected the named device. This indicates that one of the following has occurred:

1. The <device name> is not in the remote Authentication server's database.

2. The <device name> is entered incorrectly in the remote Authentication server's database.

[AUTH] RADIUS PAP rejected device: <device name>
The remote Authentication server rejected the PAP mode authentication request for the indicated device. This usually indicates that one of the following has occurred.

1. The <device name> is not in the remote Authentication server's database.

2. The device's PASSWORD did not match the password in the RADIUS server's database.

3. The RADIUS server's database entry for this device contains errors.

[AUTH] RADIUS ROUTE LOOKUP rejected IP address: <IP address>
The remote Authentication server route lookup feature rejected the IP address. This indicates that one of the following has occurred:

1. The <IP address> is not in the remote Authentication server's database.

2. The <IP address> is entered incorrectly in the remote Authentication server's database.

[AUTH] Security data buffer allocated successfully
The Authentication agent was able to allocate and initialize all memory required to perform authentication requests.

[AUTH] Security data buffer allocation failed
The Authentication agent was not able to allocate and initialize all memory required to perform authentication requests. No authentication request will be attempted. Contact your Distributor or Customer Support.

[AUTH] TACACS LOGIN rejected user: <user name>
The remote Authentication server rejected the named user. This indicates that one of the following has occurred:

1. The <user name> is not in the remote Authentication server's database.

2. The <user name> is entered incorrectly in the remote Authentication server's database.

[AUTH] TACACS No server configured for designated database location.
TACACS is configured as a database location for security authentication. Either no TACACS server has been configured or an error occurred when parsing the TACACS server configuration.

[AUTH] Warning code: 0001 Timeout
The configured authentication server(s) did not respond to requests for user authentication. Either the authentication server is not up and running, or it cannot access the IP address.

[AUTH] Warning code: 0002 Missing required attribute from server
The response message from the authentication server did not provide all required attributes for user authentication. The attributes required vary, depending on type of service, and type of security. Refer to the RADIUS Authentication Server User's Guide for details. Then check user entry for all required attributes.

[AUTH] Warning code: 0003 No UDP buffer available
Internal resources were not available to send / receive an authentication message. Contact your Distributor or Customer Support.

[AUTH] Warning code: 0004 No authentication node available
Internal resources were not available to initiate an authentication session. Contact your Distributor or Customer Support.

[AUTH] Warning code: 0005 No host configured for server IP address
The System does not have a network route to the configured authentication server(s). Verify that a static route has been set up. Then, check your configuration for the correct addresses on interfaces and authentication server.

[AUTH] Warning code: 0006 UDP system failed
Internal resources were not available to initiate an authentication session. Contact your Distributor or Customer Support.

[AUTH] Warning code: 0007 Authentication mode mismatch
An internal request for authentication server access request occurred, but the System is configured in the on-node device table mode. Contact your Distributor or Customer Support.

[AUTH] Warning code: 0008 Authentication agent not initialized
The System could not obtain enough internal resources for the user authentication operation. Contact your Distributor or Customer Support.

[AUTH] Warning code: 0009 Server failed message digest test
A message received from the authentication server did not have the correct authenticator field value.

[AUTH] Warning code: 0010 Received unexpected authentication response code from server
A message was received from an authentication server that contained an invalid response message identifier.

[AUTH] Warning code: 0011 An unexpected server responded to the access request
An access response message was received from an authentication server that is not configured in the System.

[AUTH] Warning code: 0012 UDP call back processed with no data present
A message was received from an authentication server that contained zero data bytes.

Bad auth result in smgrauth_aa_notify for device <device name>
There was no device configured (on-node or in SFVRA) for the login id entered at the user-level security prompt in the terminal server interactive window. Check configuration.

Bad context on SccDatInd <context value>
Indicates a problem has occurred in forwarding frames from the hardware to the frame relay software. The intended context for this frame is specified by the indicated context value. Contact your Distributor or Customer Support.

Bad context on X25SccDatInd <context value>
A data packet has been received with an incorrect context. This indicates that the system allocation of SCC controllers is not in a consistent state. Restart the system.

Bad FR Frame Size = <frame size>
Indicates that a frame was received with an invalid length size. Contact your Distributor or Customer Support.

Baud Rate is <value> bps
The Autobaud procedure has terminated and the RS232 port has been set to the specified baud rate.

[BIF] Could not allocate memory for buffer queue
[BIF] Initialization failed
These messages appear together in the report log. They indicate that an error occurred during initialization of the Bridge Local Interface (which is required for IP Host mode). If these messages are present in the log, the system will not operate correctly. Please contact your Distributor or Customer Support.

Booting System Software
The Second Stage Boot is attempting to load and execute the System software.

Bootstrap came alive on DM card in slot <slot #>
Informational message stating that the initialization of the Digital Modem card was successful.

Bootstrap came alive on WAN card in slot <slot #>
Informational message during a successful system initialization. Download process update for WAN card in slot <slot #>. This should be reported after the "Bootstrap loaded...waiting for response" message for a given adapter.

Bootstrap loaded on WAN card in slot <slot #>, waiting for response...
Informational message during a successful system initialization. The first of three messages providing the download process status for WAN card in slot <slot #>.

Bridge is operating in RESTRICTED mode
Bridge is operating in UNRESTRICTED mode
One of the above messages will be displayed to indicate the configured Bridge mode of operation.

Calculating CRC's.....
An X-Modem transfer has been completed and the received data is being checked for integrity.

Call control detected near end problem - Slot=<slot #> Port=<port #>
The system detected a problem when initiating a call over the indicated line. The call will be retried over a different line if possible.

Calling Line ID Failure, Duplicate ID - <calling line Id>
A call has come in for a device that is using Calling Line Id (CLID) as the only authentication method, and the given CLID is not unique across all devices.

Calling Line ID Security Failure <calling line Id>
The system has rejected a device due to a mismatch between the Calling Line Id presented by the caller and the Calling Line Id in the on-node device database or obtained via an off-node authentication server such as RADIUS.

Calling Line ID Security Failure <calling line Id>, Device: <device name>
The system has rejected a device due to a mismatch between the Calling Line Id presented by the caller and the Calling Line Id in the on-node device database or obtained via an off-node authentication server such as RADIUS. The device's name is also contained within the database.

Calling Line ID Security Failure - off-node authentication server not supported
The system authentication type is configured to obtain device information off-node, for example from a RADIUS server; however, such transactions are not yet supported when Calling Line Id Security is enabled.

Call_ID in use in HOST_CALL_REQUEST
The system software sent a message to the RBS state machine that the state machine was unable to recognize or the information was incorrect. If this message is displayed in the log messages, contact your Distributor or Customer Support.

Call Rejected, Maximum Bandwidth already in place to Device Id <device Id>
An incoming call was rejected because the Maximum Data Rate parameter was exceeded for the indicated device. The Maximum Data Rate parameter can be configured for PPP devices in SFVRA-CFG.

Call Rejected, No Called TN IE
The switch did not deliver an Information Element for the call. This problem normally occurs if you are connected to a point-to-point line and have the System configured for a multipoint line. If you are connected to a multipoint line and get this message, call your phone company and report the problem.

Call Restriction statistics reset for new day
Call Restriction device information.

Call Restriction statistics reset for new month
Call Restriction device information.

Call Restrictions will allow calls to be made this hour
Call Restriction device information.

Call Restrictions will allow calls, but this hour is restricted
Calls are restricted during this hour but the action configured is to "Warn". Calls are still being allowed.

Call Restrictions will allow calls to be made
A Call Restriction limit has been exceeded but calls will still be allowed.

Call Restrictions will no longer allow calls to be made
A Call Restriction limit has been exceeded and calls will no longer be allowed. Existing calls will NOT be forced down.

Call Restrictions will not allow calls to be made this hour
Call Restriction device information.

Call Summary for <day/month/year> - Calls/Day=x Calls/Mth=x Mins/Day=x Mins/Mth=x
Call Restriction device information. Displays daily / monthly call totals at the end of a day or a month.

Cannot make Bridge Dial Out call. No device found.
Check configuration to insure that device is properly configured.

Can only do SPEECH and 3.1K AUDIO calls in HOST_CALL_REQUEST
An improper outgoing call was attempted on an RBS line. Ensure that the device that is being called is a digital modem device and ensure that the "dm" flag has been added to peer calls.

Can't call Dial Out User. Security is not Device Level.
Check configuration. Bridge Dial Out requires device-level security and a properly configured Device List.

Can't start offnode server lookup of Dial Out User.
SmartSwitch Remote Access Module unable to send out a request to the off-node server. One of two possibilities: there may be problems communication on the LAN, or the server may not be configured properly. Verify LAN connectivity with server, and then check to see if server configured properly.

Calls Active
xx Active Sites
Current number of sites connected.

Calls Active
xxx to <sitename>
Bandwidth to each site.

Capability description processing error - <caperror>.
System is in minimal configuration mode.
A problem has occurred during system installation. The <caperror> will further identify the problem:

- *File not found*
- *Could not open file*
- *File already exists*
- *Header corruption*
- *File write problem*
- *Hash key mismatch*
- *Invalid serial number*
- *Invalid capability type*
- *Invalid capability format*
- *Invalid capability value*

The system will come up in a minimal capability mode, allowing only one physical connection, one X.25 virtual connection, and one Frame Relay virtual connection. Contact your Distributor or Customer Support.

Note: Duplicating serial numbers on all systems is a license violation.

Capability upgrade processing error - <caperror>.
Upgrade file was ignored.
A problem has occurred during system upgrade. The <caperror> will further identify the problem:

- *File not found*
- *Could not open file*
- *File already exists*
- *Header corruption*
- *File write problem*
- *Hash key mismatch*
- *Invalid serial number*
- *Invalid capability type*
- *Invalid capability format*
- *Invalid capability value*

The system will revert to its original level and the upgrade process will not be allowed. Contact your Distributor or Customer Support.

Note: Duplicating serial numbers on all systems is a license violation.

Cause <cause code> received for DLCI <dlci index>
A CLLM message was received indicating that the PVC associated with the indicated DLCI is subject to the event denoted by the indicated cause code. These events are listed below with their corresponding cause code:

Cause Code	*Event*
2	Mild congestion
3	Severe congestion
7	Fixed fault notification: facility / equipment failure
10	Discard all frames: maintenance action in progress

CB disconnect:(1) Password Incorrect
CB disconnect:(2) Call-back number not found
CB disconnect:(3) Ethernet address inconsistent
CB disconnect:(4) Disconnecting for Call-back
CB disconnect:(5) Invalid Packet Received
CB disconnect:(6) Unable to resolve protocols
CB disconnect:(7) Inband Timeout
CB disconnect:(8) Line Integrity Violation
CB disconnect:(?) Unspecified
For all of the above Combinet generated messages, the Combinet has disconnected for the indicated reason. Check your Combinet configuration, and adjust if necessary. If problem persists, contact your Combinet distributor.

[CCP] Internal Decompression Failure
The system was unable to decompress a packet though the frame was delivered properly from a protocol perspective. This is an unexpected condition with a properly functioning device implementation and is thus considered a unrecoverable error. The system will close the CCP protocol, meaning that the connection continues to operate, but in an uncompressed mode.

[CCP] Option Negotiation Failure, Non-Convergence detected
During PPP negotiation, the system attempted to negotiate CCP, but it was not possible to arrive at a mutually acceptable set of protocol parameters with the connected device. The connection continues to operate, but without compression.

The cause of this problem may result from:
- the system has too little memory to support compression, or
- the two devices involved don't agree on which bridging / routing protocol to use (due to a mis-configuration)

Check configuration for correct protocol. If this is not the problem, check memory availability.

CDR was unable to obtain a buffer to report a CDR event
A buffer was unavailable to send a call detail recording event log message, and the message was discarded. This message is logged once when the condition first occurs. It will not be logged again until the condition has been cleared and CDR has successfully obtained a buffer. If the condition occurs again later, another message will be logged.

CHANNEL in use in HOST_CALL_REQUEST
The system software sent a message to the RBS state machine that the state machine was unable to recognize or the information was incorrect. If this message is displayed in the log messages, contact your Distributor or Customer Support.

[CHAP] Authentication Failure of remote device <System_ID> - <error message>
On-node or off-node (for example, through the RADIUS Server) CHAP authentication has failed. The <*System_ID*> will contain the System ID configured in SFVRA-CFG. The <error message> will contain information that should aid in trouble shooting.

If the authentication failure is an on-node failure, the <error message> will contain one of the following strings:

Challenge Response failed hash calculation
No Secret configured in Device Table
Name not configured in Device Table
Invalid information in authentication attempt

If the authentication failure is an on-node failure, the <error message> will contain one of the following strings:

Challenge Response failed in hash calculation
No Secret configured in Device Table
Name not configured in Device Table

If the authentication failure is an off-node failure, the remote Authentication Agent will generate the error message.

[CHAP] Authentication Failure - remote device not responding
The System has not received a challenge response from the peer. The cycle is attempted the configured number of times, after which a failure is declared. Check your remote device.

[CHAP] Authentication Failure - unable to initiate server transaction <return code>
The System authentication type is configured to obtain device information off-node, for example from a RADIUS server, but an internal error has prevented the transaction from occurring. Check

the Radius Server report log for more information. If unsuccessful, contact your Distributor or Customer Support.

[CHAP] Remote device indicates Authentication Failure of system <data>
The System received a fail reply in remote CHAP mode. This means that the System has not been authenticated by the peer, and most likely the link will be released. <data> contains a portion of the received frame, which should aid in trouble shooting the situation.

Circuit-mode/Packet-mode aggregation will not be allowed,
dropping oldest connection to site <site name>
This message may appear if switched calls are used to back up Frame Relay. If this message is seen infrequently, it merely indicates the changeover from Frame Relay to switched calls and back again. If this message is seen frequently, contact your Distributor. At the same time that these messages are displayed in the log, an open Monitor Connection window may show brief periods (<1 second) where the indicated Bandwidth suddenly increases and then decreases. This is due to the changeover between Frame Relay and switched calls and is not a problem.

CNTR-TMR:Timed out waiting for TMR <number> interrupt!
The i386s specified timer did not respond during a POST testing its interrupt capabilities. The boot process should continue; however, make note of the error message in the event of a future problem.

Configured adapter #'x' type does not exist
The interface adapter indicated does not match the resource configuration in the system. Correct the configuration on the system.

Connection disconnected for license violation
A connection was disconnected because there were more connections in place than allowed with your version of the system software. A larger software version should be ordered.

Could not find port for static route with next hop address <AppleTalk Address>
Contact your distributor or Customer Support.

Could not get Call Restriction information
Contact your Distributor or Customer Support.

Could not get current monthly charges information
Could not get the current monthly call charge information on the system. The call charge feature will be disabled and the problem should be reported. Contact your Distributor or Customer Support.

Could not obtain fcr packet buffer
AppleTalk related. Contact your distributor or Customer Support.

Couldn't find speech service - <slot #, port #>
An incoming call was received which specified Speech Bearer Service capability. Speech service is not currently supported with the System. Most likely, the incoming call was a wrong number. The system will attempt to treat the call as 56 Kbps data.

Current monthly charges reset for new month
Reported on the first day of the month to indicate that the current monthly call charges value is being reset to zero.

Data link down: Slot=<slot #> Port=<port #> Ces<communication endpoint suffix>
The data link on the specified line is down. If all the data links for a line are down, the line is disabled for switched connection use.

Data link test successful: DSL <port #>, CES 1
This message applies for 1TR6 BRI only. If Layer 1 is established, a test will be done to determine if the data link can be established. This message indicates successful test results.

Data link up: Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
The data link on the specified line is active and can be used for establishing switched connections.

DCE Data Rate is invalid on FrStartPVC
The user has configured a data rate which is inconsistent with the application. This can only happen with serial lines such as V.35 where the data rate must be specified in bits-per-second and the configured rate is not valid.

Dedicated connection down: <slot #, port #>
The dedicated connection is down. Switched backup connections will be used, if available. This message will occur if the other system is down, or if the network interface line is not connected, or if the authentication of the remote device failed.

Dedicated connection to device <device name> up: <slot #>,<port #>
The indicated dedicated connection is operational.

[DHCP-P] Failed to close UDP port after terminating last DHCP client
An internal error occurred in the DHCP Proxy Client. When all DHCP client invocations are terminated, the UDP ports used by the DHCP Proxy Client should be closed. Contact your Distributor or Customer Support.

[DHCP-P] Failed to de-register with the IP Address Pool Manager, erc = <x>
This message indicates that a failure was encountered by the DHCP Proxy Client while it was being disabled. It was unsuccessful in its attempt to de-register as a provider of “DHCP” addresses for the IP Address Pool. Contact your Distributor or Customer Support.

[DHCP-P] Failed to open UDP port for first DHCP client
An internal error occurred in the DHCP Proxy Client. When the first DHCP client invocation starts, the UDP ports used by the DHCP Proxy Client should open. Contact your Distributor or Customer Support.

[DHCP-P] Failed to open UDP port (x), erc = <y>
This message appears when the DHCP Proxy Client is being enabled and it encounters an error while trying to open one or both of the UDP ports that it requires for operation. Contact your Distributor or Customer Support.

[DHCP-P] Failed to register with the IP Address Pool Manager, erc = <x>
This message indicates that a failure was encountered by the DHCP Proxy Client while it was being enabled. It was unsuccessful in its attempt to register as a provider of “DHCP” addresses for the IP Address Pool. Contact your Distributor or Customer Support.

[DHCP-P] Ignoring offers from DHCP server x.x.x.x; the server MUST be on a primary LAN interface, or IP addresses will not be obtained
In order for the DHCP proxy client to successfully obtain IP addresses for multiple interfaces, the DHCP server must reside on a primary LAN interface. If it does not, this message is written to the Report Log, and no IP addresses will be obtained from the server and placed into the IP Address Pool. To correct, use SFVRA-CFG to change the DHCP server's interface from a secondary interface into a primary interface for that LAN port.

[DHCP-P] Invalid DHCP Server LAN port encountered in configuration; NIF entry not activated
This message appears when the DHCP Proxy Client encounters an invalid configuration setting for an IP network interface's LAN port on which the DHCP server is to be reached. This will result in no IP addresses being obtained for the network interface in question. Contact your Distributor or Customer Support.

[DHCP-P] Proxy Client enabled
This message will appear whenever the DHCP Proxy Client has been successfully enabled. This message will appear during system initialization (if configuration values have enabled it).

[DHCP-P] Proxy Client initialization failed
This message indicates that the DHCP Proxy Client did not initialize successfully. The DHCP Proxy Client will not be operational. Contact your Distributor or Customer Support.

[DHCP-P] UDP port (67) opened
The DHCP Proxy Client is being enabled and it must open the BOOTPS UDP port (port 67). This message will occur during system initialization. If the DHCP Relay Agent is also enabled, it may not be necessary for the Proxy Client to open this UDP port.

[DHCP-P] UDP port (68) opened
The DHCP Proxy Client is being enabled and it must open the BOOTPC UDP port (port 68). This message will occur during system initialization.

[DHCP-R] Failed to allocate memory for transmit buffer pool
The system was unable to allocate memory for the DHCP Relay Agent's transmit buffer pool during initialization. The Relay Agent will not become operational. Contact your Distributor or Customer Support.

[DHCP-R] Failed to open UDP port (67), erc = <x>
An error occurred while attempting to enable the DHCP Relay Agent. The Relay Agent must open the BOOTPS UDP port in order to operate successfully. If this port could not be opened, the Relay Agent will not be enabled. Contact your Distributor or Customer Support.

[DHCP-R] Relay Agent enabled
The DHCP Relay Agent has been successfully enabled. This message will appear during system initialization (if configuration values have enabled it).

[DHCP-R] Relay Agent initialization failed
This message indicates that the DHCP Relay Agent did not initialize successfully. The Relay Agent will not be operational. Contact your Distributor or Customer Support.

[DHCP-R] UDP port (67) opened
The DHCP Relay Agent is being enabled and it must open the BOOTPS UDP port (port 67). This may occur during system initialization. If the DHCP Proxy Client is also enabled, it may not be necessary for the Relay Agent to open this UDP port.

Dial Out Device does not have Bridge Callable Enabled
Check configuration. Enable the *Make Calls for Bridge Data* field under *Bridging* when editing a connection protocol.

Discrepancy in dynamically-obtained device data
The System authentication type is configured to obtain device information off-node. In an outbound call scenario with security enabled, two transactions may occur for the same device. If these do not yield the same information, the call is dropped. Contact your Distributor or Customer Support.

DL <slot #, port #, ces> Down
The specified data link for a line is down and considered unusable. Refer to the log error messages for further information (`dr` command).

DM card in slot <slot #> has no firmware
While attempting to initialize the Digital Modem card, the system registered an invalid firmware state. Contact your distributor or Customer Support. You most likely need to replace or upgrade the firmware on the Digital Modem.

DM card failed FLASH download bad xx SREC
The Digital Modem card has failed the firmware update due to a corrupt file. Contact your Distributor or Customer Support.

DM card in slot <slot #> has bad FLASH
The FLASH memory on the Digital Modem card has been identified as bad during an attempt to update or access it. Contact your Distributor or Customer Support.

DM card in slot <slot #> in unknown state
The Digital Modem card is in an unrecognizable state. Reseat the card in its ISA slot, and / or check the MVIP cabling. If the problem persists, contact your Distributor or Customer Support.

DM card in slot <slot #> is not functional
The system was unable to initialize the Digital Modem in the specified slot correctly. Check all switch and / or jumper settings on the board to ensure they match the values in SFVRA-CFG. If the board is configured properly, and this message still appears, contact your Distributor or Customer Support.

DM card in slot <slot #> will receive new firmware
Informational message stating that the system has detected that the current firmware of the specified modem is a lower revision level than what is supported in the currently installed software. For 56K modem technology, the system will attempt to update the card. For modem technology other than 56K, the upgrade command must be used to upgrade the firmware revision. Watch for subsequent log messages to ensure the update is successful.

DM card in slot <slot #> failed FLASH download
The system has failed to successfully update the firmware revision of the Digital Modem card. Contact your Distributor or Customer Support.

DM card in slot <slot #> FLASH download complete
Informational message stating that the system has successfully updated the firmware present on the Digital Modem card.

DM card in slot <slot #> signals it is operational
Informational message stating that the Digital Modem is now ready for use.

DM card type configured in slot <slot #> does not exist
Using the resource database, the system has tried to initialize a Digital Modem card that doesn't exist. Check all switch and/or jumper settings on the board to ensure they match the values in SFVRA-CFG. If the board is configured properly, and the message still appears, contact your Distributor or Customer Support.

DM card in slot <slot #> will not come out of reset
There are problems initializing the board. Contact your Distributor or Customer Support.

DM upgrade timeout. Board=<board #>, Modem=<modem #>
DM upgrade error during download. Modem says = xxx
DM upgrade no response at start. Board=<board #>, Modem=<modem #>
DM upgrade flash erase failed. Board=<board #>, Modem=<modem #>
DM upgrade no response at end. Board=<board #>, Modem=<modem #>
There were problems while attempting to update the firmware of the specified modem due to either a corrupt firmware file or hardware problems. Reseat the card in its ISA slot, and/or check the MVIP cabling. If problems persist, contact your Distributor or Customer Support.

DM upgrade started. Board=<board #>, Modem=<modem #>
The system has begun to update the firmware of the specified modem on the Digital Modem card. Watch for subsequent log messages to ensure the update is successful.

DM session in unknown upgrade state. Board=<board #>, Modem=<modem #>
There were problems while attempting to update the firmware of the specified modem due to either a corrupt firmware file or hardware problems. Contact your Distributor or Customer Support.

DM upgrade success. Board=<board #>, Modem=<modem #>
The system has successfully updated the firmware of the specified modem on the Digital Modem card.

DM: TimeSlot driver circuit id already in use on CREATE
DM: No TimeSlot driver circuits available for CREATE
DM: TimeSlot driver circuit id not in use on REMOVE
DM: TimeSlot driver circuit id not found on REMOVE
There were problems related to the Digital Modem's use of the TDM bus. Contact your Distributor or Customer Support.

Downloading Bootstrap to DM card in slot <slot #>
Informational message stating that the system is attempting to initialize a Digital Modem card. Watch for subsequent log messages to ensure the initialization is successful.

Downloading DM card in slot <slot #> with operational software
Informational message displayed during a successful initialization. Watch for subsequent log messages to ensure the initialization is successful.

Downloading WAN card in slot <slot #> with operational software
Informational message during a successful system initialization. The status of the download process for WAN card in slot <slot #> is identified. This should be reported after the "Bootstrap came alive..." message for a given adapter.

DSL test failed to establish Layer 1, port=<port #>
During power up, all WAN lines undergo a test to see if Layer 1 can be established. This message indicates a test failure. Check the wiring. If correct, contact your phone company.

Duplicate Calling Line ID <Calling line Id> detected for devices <device name> and <device name>
This message is logged at system initialization if any devices are found to share duplicate Calling line Ids, and have no other authentication method. This problem should be corrected by adding additional authentication method(s) to the necessary device(s).

Each mandatory connection uses xx bytes
There is not enough memory available to accommodate the system's total capacity load. This informational message identifies how much memory is needed to add an additional mandatory connection.

Each optional connection uses xx bytes
There is not enough memory available to accommodate the system's total capacity load. This informational message identifies how much memory is needed to add an additional optional connection.

ECP negotiation failed to converge
Verify compatible encryption parameters on each side of the link.

EDRV transmit error <error code>
An error was returned upon the software's request to transmit a data frame. Contact your Distributor or Customer Support.

EDS-DES Board Absent
EDS-FEAL Board Absent
The encryption board is either physically not in the backplane, or the dip switches on the board are set incorrectly. Check for the board; verify the switch settings.

Error closing file 's'
The WAN card initialization subsystem encountered an error while downloading a WAN card. The system could not close the download disk file indicated. Restart the system. If the error continues, Contact your Distributor or Customer Support.

Error closing file <file name>, slot <slot #>
Error closing password data file
If seen repeatedly, the above messages indicate a problem with your hard drive. Please contact your Distributor or Customer Support.

Error downloading bootstrap program to adapter #'x'
The WAN card initialization subsystem encountered an error on the indicated adapter while downloading the bootstrap program. Restart the system and review the configuration for the adapter. If the problem persists, the indicated adapter card may be faulty; contact your Distributor or Customer Support.

Error downloading operational software to adapter 'x'
The WAN card initialization subsystem encountered an error on the indicated adapter while downloading operational software. Restart the system and review the configuration for the adapter. If the problem persists, the indicated adapter card may be faulty and you should contact your Distributor or Customer Support.

Error during channel initialization Access <access index>
An error has occurred during the initialization of the indicated Frame Relay Access, or port. Likely cause of this entry is that the system has run out of memory. Contact your Distributor or Customer Support.

Error during port initialization Access <access index>
An error has occurred during the initialization of the indicated Frame Relay Access, or port. Likely cause of this entry is that the system has run out of memory. Contact your Distributor or Customer Support.

Error during PVC initialization Access <access index>
An error has occurred during the initialization of the indicated. Likely cause of this entry is that the system has run out of memory. Contact your Distributor or Customer Support.

Error initializing WAN card: <WAN card Id>
The system could not initialize the specified WAN card during system initialization. Check the WAN card installation and configuration. If the error continues, report the problem.

Error in last LMI message detected Error <error code>
An error was detected in the last LMI message forwarded by the network. The error is identified by the indicated error code.

Error loading WAN board, data verify error: adapter 'x'
The WAN card initialization subsystem encountered an error during download verification. The specified adapter card may be faulty. Contact your Distributor or Customer Support.

Error mapping WAN adapter #'x' into Host memory map
The configured memory location of the indicated WAN card conflicts with another WAN card or device. Review the configuration for the indicated adapter.

Error opening file <file name>
Error opening file <file name>, section = <section name>
Error opening file <file name>, slot <slot #>
If seen repeatedly, contact your Distributor or Customer Support.

Error parsing old WAN (Direct Host) interface: bad format
The information contained in the WAN (Direct Host) interface is invalid. To correct, use SFVRA-CFG to reconfigure the interface.

Error initializing WAN card: <WAN card Id>
The system could not initialize the specified WAN card during system initialization. Check the WAN card installation and configuration. If the error continues, report the problem.

Error parsing old WAN (Direct Host) interface: LAN interface <LAN netif name> for specified port <port#> already in use
This error may display after upgrading software which contains secondary IP addressing and an "old" style WAN (Direct Host) interface. To correct, use SFVRA-CFG to delete any WAN (Direct Host) interfaces on the problematic LAN port, and reconfigure them.

Error parsing old WAN (Direct Host) interface: no LAN interface for specified port <port#>
This error may display after upgrading software which contains secondary IP addressing and an "old" style WAN (Direct Host) interface. To correct, use SFVRA-CFG to delete the problematic WAN (Direct Host) interface. Afterwards, configure a LAN interface and then read the WAN (Direct Host) interface.

Error parsing WAN (Direct Host) interface: no LAN interface for specified name <name>
The LAN network interface associated with this WAN (Direct Host) interface is not present. Use SFVRA-CFG to delete the problematic WAN (Direct Host). Check configuration for the suspect LAN interface; it most likely will not be there. Add LAN interface, then reconfigure the WAN (Direct Host) interface.

Error opening file \system\ethernt2.bin
The LAN adapter executable file could not be opened. Check for proper software installation.

Error programming adapter #'x' hardware
The WAN card initialization subsystem encountered an error while attempting to program the hardware on the indicated adapter. Restart the system and review the configuration for the adapter. If the problem persists, the indicated adapter card may be faulty; contact your Distributor or Customer Support.

Error reading file <file name>, section = <section name>
If seen repeatedly, the above message indicates a problem with your file system. Contact your Distributor or Customer Support.

Error reading file \system\ethernet2.bin,section = <file type>
The specified section of the LAN adapter executable file could not be read. Check for proper software installation.

Error reading platform type: couldn't open file C:\SYSTEM\PLATFORM.NEI
Error reading platform type: error reading C:\SYSTEM\PLATFORM.NEI
Error reading platform type: there is no "plat name" field
Error reading platform type: there was no "=" in the string
Error reading platform type: type value is too large
Error reading platform type: type was not converted to an int
There is a problem with the platform.nei file. Reinstall the system Installation/Upgrade diskettes or CD-ROM.

Error reading sdconf.rec file
An error occurred during parsing of the ACE configuration file. The file was found, but did not have the expected format. Either repeat the download of the file from the ACE server, or reenter the ACE database location configuration using SFVRA-CFG.

Error requesting slot activation
Contact your Distributor or Customer Support.

Error sending message to Call Control
The system detected a failure while sending a message to the WAN adapter. Restart the system and review the resource configuration. If the error persists, contact your Distributor or Customer Support.

Event <event code> occurred on FR Access <access index>, DLCI <dlci index>
A debug message logged to indicate Frame Relay events occurring for the indicated DLCI on the indicated Access. The event is given in both textual, event, and numeric, code, forms.

Facility not subscribed - Slot=<slot #> Port=<port #>
This probably indicates a SPID configuration error on the indicated line. The configuration should be corrected on the system or the switch.

Failed to allocate enough memory for XILINX load file
The WAN card initialization subsystem failed to allocate a buffer for use in downloading files. Restart the system. If the problem continues, contact your Distributor or Customer Support.

FAILED TO BOOT SYSTEM SOFTWARE
While attempting to load the System software, an error was detected. The system will automatically reset and attempt a reboot in an effort to correct the problem. If the system continues to fail, make note of the displayed messages, and contact your Distributor or Customer Support. A software update is likely needed.

FAILED TO FORMAT RFA
The Flash File System could not be formatted. The system will automatically reset and attempt a reboot in an effort to correct the problem. If the system continues to fail, make note of the displayed messages, and contact your Distributor or Customer Support. A software update is likely needed.

FAILED TO INSTALL XMODEM FILESET INTO FLASH MEMORY
While writing a file into the Flash File System, an error was detected. The system will automatically reset and attempt a reboot in an effort to correct the problem. If the system continues to fail, make note of the displayed messages, and contact your Distributor or Customer Support. A software update is likely needed.

Failed to obtain Terminal info in smgr_proc_terminal_auth_sess 0
A session control block was not found for this authentication session. Contact your Distributor or Customer Support.

Failed to start a Terminal Auth session. Device + User level Security not enabled
A terminal mode connection was received and Device + User level security was not enabled. Verify correct security settings and default async protocol settings.

FAILED XMODEM INITIALIZATION
The UART controlling the Console Information Port (CIP) could not be initialized. The system will automatically reset and attempt a reboot in an effort to correct the problem. If the system continues to fail, make note of the displayed messages, and contact your Distributor or Customer Support. A software update is likely needed.

FAILED XMODEM SESSION
The X-Modem session did not successfully terminate. Likely causes include exhausting timeout limits and noisy lines. The system will automatically reset and attempt a reboot in an effort to correct the problem. If the system continues to fail, make note of the displayed messages, and contact your Distributor or Customer Support. A software update is likely needed.

Failure during read of file <file name> for WAN card in slot <slot #>
If seen repeatedly, the above message indicates a problem with your hard drive. Contact your Distributor or Customer Support.

Failure during read of file 's'
The WAN card initialization subsystem encountered an error reading the file indicated. Check for proper software installation.

Failure during Static RAM test on adapter #'x'
The WAN card bootstrap program encountered an error during the Static RAM test. This indicates that the adapter card may be faulty. Contact your Distributor or Customer Support.

Failure on closure of file <file name>
Failure on file closure <file name>
Failure on write of file <file name>
Failure opening file <file name>
If seen repeatedly, the above messages indicate a problem with your hard drive. Contact your Distributor or Customer Support.

Failure to allocate enough memory for XILINX load file
The WAN card initialization subsystem failed to allocate a buffer for use in downloading files. Restart the system. Report the problem if it continues.

File=l2, Fn=<func name>, err=Layer 2 Error<err msg>, port=<port#>, CES=<link Id>
A Layer 2 error was encountered on the indicated BRI link or port. Your ISDN line (data link) may be going down. If this error condition persists, contact your Distributor or Customer Support. Below are possible error messages and their corresponding definitions:

DISC rcvd
The Network has sent a Layer 2 DISC (Disconnect), terminating the data link. An attempt will be made to re-establish the data link after a switchtype-dependent delay.

DM rcvd
The Network will not allow establishment of the data link at this time. An attempt will be made to re-establish the data link after a switchtype dependent delay.

MDL_ERR_RESP rcvd
The Network has not responded to TEI requests - no data link was established. An attempt will be made to re-establish the data link after a switchtype dependent delay.

rcvd MDL_REM_REQ for TEI <TEI value>
The network has removed the specified TEI, terminating the data link. An attempt will be made to re-establish the data link after a switchtype dependent delay.

File=ME, Fn=_mdl_err, err=Layer 2 Error<err code>rcvd, port=<port#>, CES<link Id>
A Layer 2 error was encountered on the indicated BRI link or port. Your ISDN line (data link) may be going down. If this error condition persists, then report the problem. Below are possible error codes and their corresponding definitions (based on Table 11-1 from CCITT Q.921 specification):

A
The Network sent a RNR (Receiver not Read) or REJ (Reject).

B, D
The Network sent a DM(F=1) or a UA and will not allow establishment of the data link at this time. An attempt will be made to re-establish the data link after a switchtype dependent delay.

C
The Network sent an unsolicited UA and will not allow establishment of the data link at this time. An attempt will be made to re-establish the data link after a switchtype dependent delay.

E
The Network sent a DM(F=0). The data link will be restarted immediately.

F
Network restarted data link.

H
Timeout on sending DISConnect to the Network. Unable to bring up data link. An attempt will be made to re-establish the data link after a switchtype dependent delay.

I
Timeout sending I(Info) frame to the Network. The data link will be restarted immediately.

J
The Network sent a Layer 2 frame with an incorrect receive sequence number (Nr).

K
The Network sent a FRMR (Frame Reject) response. The data link will be restarted immediately.

L
The Network sent a Layer 2 frame with a control field error. This is typically an unimplemented frame.

M
The Network sent a Layer 2 frame with an illegal Info field.

N
The Network sent a Layer 2 frame with an incorrect length.

O
The Network sent a Layer 2 frame that was too long.

U
The Network sent a Layer 2 frame with a control field error. Typically an unknown frame.

File Access Err
System unable to access file. Check for one of the following log error messages:

```
Error opening file <file name>
Error reading file <file name>, section = <section name>
Error opening file <file name>, slot <slot #>
Read 0 bytes from file <file name> for WAN card in slot <slot #>
Failure during read of file <file name> for WAN card in slot <slot #>
Error closing file <file name>, slot <slot #>
Error closing password data file
Error opening password data file
Failure on closure of file <file name>
Failure opening file <file name>
Failure on file closure <file name>
Failure on write of file <file name>
```

If you see any of these log messages repeatedly, there may be a problem with the file system. Contact your Distributor or Customer Support.

Formatting Flash Memory.....
The user has either requested the Flash to be formatted or a corrupted Flash File System was detected while attempting to save an upgrade/installation file set (transferred via X-Modem).

[FR_IETF] Authentication Failure of remote device NAME
[FR_IETF] Off-Node Authentication Failure of remote device NAME
The device database does not contain an entry for the device specified by NAME. Reconfigure either the PVC name or the device name so that they match.

[FR_IETF] detected PPP protocol from "NAME", shutting down PVC
FR_IETF has detected a configuration mismatch between the system and the remote device NAME. The administrator must change the PVC configuration on one of the devices.

Frame Relay event queue full
Indicates a lack of system resources to handle the level of traffic being experienced. Contact your Distributor or Customer Support.

Frame Relay PVC connection down: Slot=<slot number>, Port=<port number>
The Frame Relay PVC connection is down for the indicated slot and port number.

Frame Relay PVC connection up: Slot=<slot number>, Port=<port number>, DLCI=<DLCI index>
The Frame Relay PVC connection is up for the indicated slot, port, and DLCI index.

FrBufFree: error <error code> during free
The indicated error occurred during an attempt to free a buffer to its memory pool. Contact your Distributor or Customer Support.

FrUtl: No registered device for DLCI <dlci index>
A frame was received on the PVC associated with the indicated DLCI, and no Frame Relay Service Device had (as yet) registered to use this PVC.

IePvcStatus: Received Status Report for unknown PVC # <dlci index>
The indicated unknown DLCI was indicated in a STATUS message received from the network. This DLCI number is entered in the "unknown DLCI" list and can be displayed via the FR LMI system console command.

Incoming call from <Device Name>, Slot=<slot #>, Port=<port #>, Chan=<channel #> Rejected by BW Reservation
A bandwidth reservation message. Indicates that a call has come in from the indicated device, on a line that is not in this device's profile. The call will be disconnected. If you see this message often, check the remote device's configuration to prevent wasted calls.

Initial TDM Clock Master: <slot#, line#>
The external line indicated has been selected as the master clock source.

Initializing...
Displays the current state of the system (initialization).

Installing File Set into Flash Memory
The file set, received via X-Modem, has successfully passed its verification tests and is now being written into the Flash File System.

Insufficient space for buffer pool creation
There is not enough system memory to proceed with the creation of the requested size buffer pool. Contact your Distributor or Customer Support.

Interrupt fault on WAN Adapter in Slot <slot #>
The interrupt jumper for the WAN Adapter in the specified slot is missing or misplaced.

Invalid caller number: <caller's sites name> - <caller's number>
The incoming call security feature is enabled and a call was received from an unknown remote site, therefore the call was disconnected. If the call was from a valid remote site, the device list must be updated to include the remote site's phone number.

Invalid Call_ID in HOST_CALL_CONNECTED
Invalid Call_ID in HOST_CALL_DISCONNECT
The above Robbed Bit Signaling messages indicate that the system software sent a message to the RBS state machine that the state machine was unable to recognize or the information was incorrect. If this message is displayed in the log messages, contact your Distributor or Customer Support.

Invalid CLLM received on Access <access index>
An invalid CLLM message was received on the indicated Frame Relay Access. The message had either missing elements or invalid contents.

Invalid LAN Adapter identifier
The system has detected invalid LAN adapter hardware. Check for proper LAN adapter configuration and hardware installation.

Invalid Password <password> given
The remote Combinet sent a password that did not match any device table entries. This most likely is due to a configuration error. Check the configuration, and change the password.

Invalid SERIAL.001 file present, file is ignored.
Contact your Distributor or Customer Support.

Invalid SERIAL.BIN file present, system booting in minimal mode.
Contact your Distributor or Customer Support.

Invalid serial number in SERIAL.001, file is ignored.
Contact your Distributor or Customer Support.

Invalid serial number in SERIAL.BIN file, system booting in minimal mode.
Contact your Distributor or Customer Support.

IP Error from ESP datagram - discarded
An error occurred within the IP forwarding logic which make it impossible to send this datagram.
[IP] Invalid Device Info. Device is not IP callable <device name>
An IP packet could not be forwarded to a remote network because the next-hop device for that network is not configured as *IP Callable*. The SmartSwitch Remote Access Module returns a *network unreachable* message to the sender.

[IP] x.x.x.x not added to the pool: Invalid IP address
A failure was encountered by the IP subsystem during initialization processing. IP made an unsuccessful attempt to add a “static” address to the IP Address Pool. The IP address being added did not match any of the configured IP network interfaces.

[IP] x.x.x.x not added to the pool: Invalid Device Id
A failure was encountered by the IP subsystem during initialization processing. IP made an unsuccessful attempt to add a “static” address to the IP Address Pool. The ID supplied by the IP subsystem was invalid. Contact your Distributor or Customer Support.

[IP] x.x.x.x not added to the pool: IP Address Pool Full
A failure was encountered by the IP subsystem during initialization processing. IP made an unsuccessful attempt to add a “static” address to the IP Address Pool. The IP Address Pool was already full.

[IP] x.x.x.x not added to the pool: Unknown error (y)
A failure was encountered by the IP subsystem during initialization processing. IP made an unsuccessful attempt to add a “static” address to the IP Address Pool. An unknown error code was returned by the IP Address Pool Manager. Contact your Distributor or Customer Support.

[IPAP] ResMem returned invalid device maximum value (x)
A memory allocation failure was encountered by the IP Address Pool Manager during initialization processing. Contact your Distributor or Customer Support.

[IP] Cannot get system memory for xxxx
There is not enough system memory available for IP software to operate (“xxxx” is a variable name internally used). Contact your Distributor or Customer Support.

[IP] Cannot process incoming remote IP device <IP address>, no rsc avail
The IP software was unable to accept the incoming IP device to a WAN (Direct Host) interface because it could not obtain necessary resource. The WAN connection may remain for a while, but the remote IP device will not be able to communicate with any IP devices over WAN. Contact your Distributor or Customer Support.

[IP] Cannot start Proxy Arp for <IP address #>, no cmd buf avail
The IP software attempted to start the proxy arp for the IP device indicated by the <IP address #>, but was unsuccessful because it could not obtain necessary memory. Contact your Distributor or Customer Support.

[IP] Cannot stop Proxy Arp for <IP address #>, no cmd buf avail
The IP software attempted to stop the proxy arp for the IP device indicated by the <IP address #>, but was unsuccessful because it could not obtain necessary memory. Contact your Distributor or Customer Support.

[IP] Datagram with destination address of <destination address> cannot be forwarded
[IP] Reason: Invalid Device Info. Device <device name> is not IP callable
These two message appear together if a user calls in to the specified destination user and that user is not configured to be IP callable.

[IP] Default Route not added, invalid next hop (<IP address #>)
Because of an incorrect setup, the default route entry was not added in the routing table. Check the next hop in your configuration. Be sure that the next hop indicated by the <IP address #> is directly connected to the configured network interface.

[IP] Failed to de-register with IP Address Pool Manager (erc=x)
A failure was encountered by the IP subsystem during initialization processing. IP made an unsuccessful attempt to de-register as a provider of "static" addresses for the IP address pool. Contact your Distributor or Customer Support.

[IP] Failed to register with IP Address Pool Manager (erc=x)
A failure was encountered by the IP subsystem during initialization processing. IP made an unsuccessful attempt to register as a provider of "static" addresses for the IP address pool. Contact your Distributor or Customer Support.

[IP] Initialization failure
The IP Router was not initialized correctly because of other errors. Possible errors include "[IP] Cannot get system memory for xxxx". Refer to the log for additional messages to pinpoint the problem.

[IP] Invalid configuration for Network Interface dd
IP routing is not properly configured. Refer to the *IP Network Interfaces* section of the Central Site CSX user documentation to verify.

[IP] Invalid RLAN IP Address <IP address>, RLAN IP Stream Closed
The connection from a HDLC Bridge or a PPP device came up and the IP (sub-) network number configured for it is invalid; it does not belong to any of the WAN (RLAN) interfaces. Correct the IP address for the remote device.

[IP] Invalid Peer IP Address <IP address>, WAN IP Stream Closed
A PPP or RFC 1294 (IP Host) connection came up, and the IP address of the peer device (pre-configured or negotiated) belongs to a WAN (RLAN) Interface. If the IP address is preconfigured, try changing the peer's IP address (at the peer device and possibly on the device entry for the peer) that belongs to one of the WAN, WAN (Direct Host), or WAN (UnNumbered) interfaces. If the IP address is negotiated, try changing the IP address pool, or make sure that you really do want to use a WAN (RLAN) Interface.

[IP] IP host is initialized successfully
This message is posted when the system IP Host feature has initialized successfully.

[IP] IP router is initialized successfully
This message is posted when the system IP Router feature has initialized successfully.

[IP] Network initialized successfully on ddd.ddd.ddd.ddd
This message is posted when the numbered interface is successfully initialized on the indicated IP address.

[IP] Network Interface on LAN port <port #> already exists
There is another network interface that is configured for the LAN port indicated, and it was already initialized successfully. This means that there are multiple network interfaces configured for the same LAN port. You should correct the system configuration.

[IP] Network Interface on LAN port <port #> not initialized
The network interface for the LAN port indicated was not initialized because there is no Ethernet resource configured, or the Ethernet resource that is configured does not have the corresponding port. You should correct the system configuration.

[IP] Route (<IP address #1>) not added, invalid next hop (<IP address #2>)
The static route entry indicated by the <IP address #1> was not added in the routing table because the next hop indicated by the <IP address #2> is not located on any network directly connected to the configured network interface.

IPSec - Duplicate SA, Final Dest Addr: nn.nn.nn.nn SPI nn.nn.nn.nn
A Security Association with the same SPI and Final Destination Address already exists. If there is no SPI parameter listed, the Security Association table has been filled.

IPSec Security Associations initialized successfully

[IP] WAN (Direct Host) Interface for LAN port <port #> already exists
There is another WAN (Direct Host) type interface that is configured for the LAN port indicated, and it was already initialized successfully. This means that there are multiple WAN (Direct Host) type interfaces configured for the same LAN port. Use SFVRA-CFG to specify primary or secondary interface.

[IP] WAN (Direct Host) Interface <WAN interface name>, invalid associated LAN interface <LAN interface name>
The WAN (Direct Host) type interface could not come up; the associated LAN network interface, specified by configuration, was not found. Use SFVRA-CFG to delete old WAN (Direct Host) interface. Check for associated LAN interface, and add if necessary. Then add back the WAN (Direct Host) interface.

[IP] WAN (Direct Host) Interface for network <network #> on LAN port <port #> initialized successfully
This message is posted when WAN (Direct Host) interface for the indicated network is initialized successfully.

[IPCP] Invalid pre-configured IP address <IP address> for <device name>, ignored
There is a configured IP address for the remote device in the Device Table, but the IP address does not belong to any configured WAN interfaces. Check the configuration. You will most likely need to add another WAN interface.

[IPCP] IP Address Pool - Out of IP addresses
IPCP needed to allocate an IP address from the IP address pool, but there were no IP addresses available in the IP address pool. You may need to add more IP addresses to the pool.

[IPCP] Option Negotiation Failure, Non-Convergence detected
IPCP is terminated because an agreement could not be reached on the details of protocol. Refer to the specific documentation for the device in question to determine if it is configured correctly. Then, contact your Distributor or Customer Support.

[IPCP] Remote device does not negotiate IP address
Please configure IP address for the device <device name>
The IP address for the remote device is either improperly configured, or not configured at all. Check configuration and adjust.

[IPFILT] Filter "abcd" does not exist, ignored by application point "xyz"
This particular error message detects that an attempt has been made to apply a non-existent filter. In theory, this can only happen if someone manually modifies a configuration file (other than through SFVRA-CFG).

[IP Host] Call Dropped: ID Response was not received from remote
The system did not receive a valid identification exchange from the remote IP Host. The system has rejected the incoming call. Refer to the *Quick Start* for proper setup of your particular device.

[IP Host] Call Dropped: XID was not received from remote
The system did not receive a valid identification exchange from the remote IP Host. The system has rejected the incoming call. Refer to the *Quick Start*.

[IP Host] Security Rejection - Digit string wrong length
The system did not receive a valid identification exchange from the remote IP Host. The Identification digit string from the remote device was not of an appropriate length. This string must be a 24 character string of ASCII digits (0-9), which is blank padded. The system has rejected the incoming call.

[IP Host] Security Rejection - Invalid Security ID <Id string>
The system has received an IP Host Id, <Id string>, from a remote device that is not configured in the Device List. The system has rejected the incoming call. Verify that the IP Host ID in the Device List information is identical to the IP Host Id configured in the remote device.

[IP Host] Security Rejection - Security ID cannot be validated with Authentication Server
The System authentication type is configured to obtain device information off-node, for example from a RADIUS server; however, such transactions are not yet supported when IP Host ID Security is enabled.

[IP RIP] All network interfaces used
All RIP interface data structures are in use. No RIP information will be sent to any additional interfaces. Contact your Distributor or Customer Support.

[IP RIP] Buffers allocated
The RIP successfully allocated the UDP buffers needed to transmit RIP packets.

[IP RIP] Initialization failed, unable to allocate buffers
The RIP initialization was not completed. The machine contains insufficient memory to allocate the UDP buffers needed to transmit RIP packets. Contact your Distributor or Customer Support.

[IP RIP] RIP Protocol Initialization successful
The RIP protocol was successfully initialized.

[IP RIP] Route Maintenance Registration Failed
The IP RIP protocol was unable to register with the IP routing table notification system. Any dynamic changes of the routing table configuration will not be reflected in the RIP packets sent to other routes. contact your Distributor or Customer Support.

[IP RIP] Send queue full
The RIP transmission queue has become full. This is not a normal occurrence. The machine should be restarted. If this message is displayed again after the machine has been restarted, contact your Distributor or Customer Support.

[IP RIP] Unable to add host route <IP address>
A failed attempt was made to add the host route to the IP RIP routing table. The routing table can have approximately 300 routing entries, and at this time, the routing table is full. The host route will not be broadcast via RIP packets and therefore other routers will not be able to learn the route to this device. You can use the packet capture commands to try to determine if a device is advertising an unusual number of routes. If you are unable to track down the problem, contact your Distributor or Customer Support.

[IP RIP] Unable to add route, routing table full
The IP RIP routing table is currently full, no new routes can be added. The routing table can have approximately 300 routing entries, and at this time, the routing table is full. This could result in possible unreachable destinations. You can use the packet capture commands to try to determine if a device is advertising an unusual number of routes. If you are unable to track down the problem, contact your Distributor or Customer Support.

[IP RIP] Unable to open RIP/UDP port 520
The UDP port for RIP was unable to be opened. There are 63 possible UDP ports, and none are available for use at this time. No RIP information can be transmitted or received. Contact your Distributor or Customer Support.

[IP RIP] Unable to register WAN Connection notification
The IP RIP protocol was unable to register with the IP WAN interface connection notification system. No WAN connection information will be reflected in the RIP packets. Contact your Distributor or Customer Support.

[IP RIP] Unable to register with Network Interface Maintenance
The IP RIP protocol was unable to register with the IP network interface notification system. Contact your Distributor or Customer Support.

[IPX] Invalid IPXWC passed
In the unlikely event this message is posted, contact your Distributor or Customer Support.

[IPX] Network initialized successfully on xxxxxxxx:xxxxxxxxxxxx
This message is posted when the numbered interface is successfully initialized on the indicated IPX address.

[IPX] Network Interface on LAN port <port #> not initialized
The network interface for the LAN port indicated was not initialized because there is no Ethernet resource configured, or the Ethernet resource that is configured does not have the corresponding port. You should correct the system configuration.

[IPX] Route <IPX network address #1> not added: invalid next hop(<IPX address #2>
The static route entry indicated by the <IPX network address #1> was not added in the IPX routing table because the next hop indicated by the <IPX address #2> is not located on any network directly connected to the configured network interface.

[IPX] Route (<IPX network address>) not added: invalid next hop (<name>)
The static route entry indicated by the <IPX network address> was not added in the IPX routing table because the next hop remote device indicated by the <name> does not exist.

[IPX] IPX router initialized successfully
This message is posted when the IPX Router feature has initialized successfully.

IPX spoofing unable to get disconnect time structure. Default options replacing disconnect time options for device <device name>.
The resources required to properly perform the configured IPX spoofing options for the specified device after a connection to this device has been disconnected could not be obtained. The default IPX spoofing options are being used in place of the disconnect time IPX spoofing options.

[IPX RIP] Buffers allocated
The IPX RIP successfully allocated the buffers needed to transmit IPX RIP packets.

[IPX RIP] RIP Protocol Initialization successful
The IPX RIP protocol was successfully initialized.

[IPX RIP] Space available in routing table
A route entry has become available in the full route table.

[IPX RIP] Unable to add route, routing table full
The route table has become full. The maximum number of route entries should be increased. Note: This message will not recur in the log until space becomes available in the route table.

[IPX SAP] Buffers allocated
The IPX SAP successfully allocated the buffers needed to transmit IPX SAP packets.

[IPX SAP] SAP Protocol Initialization successful
The IPX SAP protocol was successfully initialized.

[IPX SAP] Space available in service table
A service entry has become available in the full service table.

[IPX SAP] Unable to add service, service table full
The service table has become full. The maximum number of service entries should be increased.
Note: This message will not recur in the log until space becomes available in the service table.

[IPXCP] Add Network Address to Pool with value above <network address>
This message informs the administrator that negotiation was not possible since non-convergence was detected the network address sent by the peer was not acceptable by us and we do not have any network address to assign to the peer. The possible remedy is to configure more IPX addresses with a value more than <Network Address> in the Address Pool.

[IPXCP] IPX Address Match.
[IPXCP] Device <device> address same as another device address
The remote device indicated by <device> requested to use an already existing IPX network number and node number.

[IPXCP] Our Node Address is <node address>
This message informs the administrator that the peer has assigned us a node number because the system did not have a node address and the peer needs a node address. This node address will be used by the peer to identify this system.

[IPXWAN] Master Slave Conflict. Change Internal Network Number above <present value>
This message indicates that over the IPXWAN link, the master and slave roles could not be determined. The internal network number of the system must be changed to ensure proper IPXWAN negotiation to occur.

[IPXWAN] IPX Internal Network Number must be configured.
You must configure a valid internal network number in order for IPX routing to work properly.

L3_CallRefSelect Call Reference wrapped
Status message indicating that Layer 3's call reference value has wrapped. If this message is posted frequently, report the problem.

LAN Adapter Abort
The Ethernet adapter or subsystem is being interrupted as part of the error recovery process. If the system fails to operate normally, or the warning continues to occur, then report the event using the problem reporting form included in *Getting Assistance*.

LAN Adapter Command Timeout
The system expected a command from the LAN adapter or subsystem that it did not receive. Check for proper LAN adapter configuration and hardware installation. If it persists, report the event using the problem reporting form included in *Getting Assistance.*

LAN Adapter configuration conflict
There is a configuration conflict between the Ethernet resource that was installed and the Ethernet resource that was configured. Correct the configuration to match the installation.

LAN Adapter Fatal Error Reported
LAN Adapter hardware failure detected. If the problem persists, replace your LAN adapter.

LAN Adapter FIFO Data Underrun
The system expected data from the adapter that it did not receive, and the system will continue to operate. Check for proper LAN adapter configuration and hardware installation.

LAN Adapter FIFO not empty, status=<status value>
The LAN adapter did not enter the proper state after it was restarted. Check for proper LAN adapter configuration and hardware installation.

LAN Adapter HW upgrade may be required
Older versions of the Ethernet adapter may need to be updated to run Release 2.3 or greater. If the above message appears in your system log messages, you will need to remove your Ethernet adapter to determine if it is a version that needs to be updated. Refer to the "Notes and Warnings" section of the Release Notes for further instructions.

LAN Adapter HW upgrade required
Older versions of the Ethernet adapter may need to be updated to run Release 2.3 or greater. If the above message appears in your system log messages, you will need to upgrade your Ethernet adapter.

LAN Adapter LAN Controller error
The system detected an error with the LAN controller. The LAN adapter card may be faulty. Contact your Distributor or Customer Support.

LAN Adapter not configured
The system tried to access the bridging function when it was not configured. Most likely, the Ethernet resource was accidentally deleted. Correct the system configuration to reflect the proper Ethernet resource.

LAN Adapter out of receive buffers for LAN port <port #>
The LAN adapter is temporarily out of receive buffers for the indicated port. This condition should clear itself. If the condition persists, contact your Distributor or Customer Support.

LAN Adapter out of receive buffers for the WAN port
The LAN adapter is temporarily out of the buffers it uses to receive packets from the WAN port. This condition should clear itself. If the condition persists, contact your Distributor or Customer Support.

LAN Adapter port <port #> transmit error <error code>, check connection
The LAN adapter detected an error transmitting a frame on the indicated port. Check that the LAN is properly connected to the adapter and that the LAN is properly terminated.

LAN Adapter Reset
This is an initialization message. The Ethernet adapter has been reset as part of the adapter initialization sequence.

LAN Adapter Response Timeout
The system expected a command response from the adapter that it did not receive. Check for proper hardware installation.

LAN Adapter ROM version ########.########.########
The ROM version in the Ethernet adapter is indicated.

LAN Adapter software version conflict
When software is downloaded onto the Ethernet adapter, its software version is compared to the version of software running on the host's main processor. If the versions do not match, this message is posted. The upgrade did not work properly; contact your Distributor or Customer Support.

LAN Adapter System resource error
LAN Adapter hardware failure detected. If the problem persists, replace your LAN adapter.

LAN Init Error
LAN connection failure. Initialization failure detected by the LAN packet forwarding component in the system.

LAN Port <port #> detected a transceiver problem
The system detected a LAN connection problem on the indicated port. Check for proper LAN connection installation.

LAN Port <port #> detected jabber condition <n> times(s)
A "jabber" condition or an Ethernet frame larger than the maximum legal length has been received. This message is usually displayed if there is a malfunctioning transceiver or a malfunctioning Ethernet device on the LAN. This message is not displayed for every error condition. It appears after 24 hours since the last message was displayed. This message provides the LAN port # in question, and the number of times <n> the jabber condition has been detected.

LAN Port <port #> detected open LAN media
The system detected a problem with the physical LAN on the indicated port. The LAN is not properly terminated or the LAN is not fully connected to the system. Check for proper LAN installation.

LAN Port <port #> detected shorted LAN media
The system detected a problem with the physical LAN on the indicated port. The LAN is not properly terminated or the LAN is not fully connected to the system. Check for proper LAN installation.

LAN Port <port #> is now in the Forwarding state
The bridge LAN port indicated has entered the forwarding state and is now ready for data transfer.

LAN Port <port #> is now in the Learning state
The bridge LAN port indicated has entered the specified state.

LAN Port is now in the Listening state
The bridge LAN port is entering the specified state.

LAN Port <port #> is now in the <new state> state
The bridge LAN port indicated is entering the specified new state.

LAN Xmit Error
LAN connection failure. LAN packet transmit error detected by the system.

Layer 1 sync not seen - Slot=<slot #> Port=<port#> Ces=<communication endpoint suffix
A physical problem has been detected on the indicated line. Check for proper connection to the SmartSwitch Remote Access Module and to the NT1 or CIU. If the NT1 or CIU appears functioning properly, call your phone company and report the problem.

[LCP] Option Negotiation Failure, Non-Convergence detected
Link Control Protocol is terminated because the SmartSwitch Remote Access Module and the device cannot agree on a common way of communicating. The device may not be configured properly. Refer to the specific documentation for device set up. Then, contact your Distributor or Customer Support.

Line <slot #, port #> Down
ISDN line failure. The data link for the line connected to slot <slot #> port <port #> is down.

LMI alarm on Access <access index>
Indicates that either no STATUS messages have been received from the network or that N393 errors have occurred in the last N391 events thus exceeding the device configured alarm threshold for the LMI link. Any associated PVCs are disabled. (The variable N393 is the configured Monitored Events Count, and the variable N391 is the configured Full Status Enquiry Polling Count.)

LMI alarm reset Access <access index>
Indicates that N392 events have occurred which allows the LMI alarm condition to be cleared and any associated PVCs to be re-enabled. (The variable N392 is the configured Error Threshold Count.)

Loop detected on Local Area Network
The LAN adapter has detected a loop condition on the local area network. The system will discard these frames until the loop condition is removed.

MAC Layer Bridge did not Initialize
A system problem prevented the MAC layer bridge from properly initializing, and the bridge will not forward data over the WAN. Restart the system. If the error continues, contact your Distributor or Customer Support.

Manual intervention required: please replace LAN card
Older versions of the Ethernet adapter may need to be updated or replaced to run Release 2.3 or greater. If the above message appears in your system log messages, you will need to replace your Ethernet adapter.

Manual restart initiated on DM board in slot <slot #>
There was an attempt to restart the specified Digital Modem with the `modem restart` command. Check subsequent log messages to verify the command was successful.

Maximum call charges exceeded for month
The configured maximum for monthly call charges has been exceeded.

Maximum call minutes per day limit (x) has been reached
The described limit has been exceeded. The next log message will indicate whether calls will still be allowed or not.

Maximum call minutes per month limit (x) has been reached
The described limit has been exceeded. The next log message will indicate whether calls will still be allowed or not.

Maximum calls per day limit (x) has been reached
The described limit has been exceeded. The next log message will indicate whether calls will still be allowed or not.

Maximum calls per month limit (x) has been reached
The described limit has been exceeded. The next log message will indicate whether calls will still be allowed or not.

MCP detected channel failure: <channel number>
A link has failed for some abnormal reason and the indicated channel has been disconnected. This message is generally preceded by another message which indicates the underlying protocol. Refer to that message. If this does not pinpoint the problem, check the application on the remote device to see if it is working correctly.

Memory Access Timeout
This indicates a TDM bus connector failure that is specific to the TDM bus connecting a primary rate and a basic rate adapter. Ensure that the TDM bus has been correctly connected to the two adapters. If problem continues, contact your Distributor or Customer Support.

MEMORY LIMITED - <x> COMPRESSION connections available
Where "x" is equal to the number of connections that can be supported. There is not enough memory available to support the number of compression connections being allocated. You may want to purchase more memory for your system. Contact your Distributor or Customer Support.

Mild congestion CLLM received for DLCI <dlci index>
A CLLM message was received indicating mild congestion may be expected on the PVC associated with the indicated DLCI.

Mismatch of configured and installed DM card in slot <slot #>
The switch and / or jumper settings on the specified Digital Modem card are not properly set to match how the card is configured in software. Check the hardware and software configuration and restart.

Missing BEARER_CAPABILITY in HOST_CALL_REQUEST
Missing CALLED_NUMBER_IE in HOST_CALL_REQUEST
Missing CHANNEL in HOST_CALL_REQUEST
Missing CHANNEL_ID_IE in HOST_CALL_REQUEST
Missing TN in HOST_CALL_REQUEST
The above Robbed Bit Signaling messages indicate that the system software sent a message to the RBS state machine that the state machine was unable to recognize or the information was incorrect. If this message is displayed in the log messages, contact your Distributor or Customer Support.

MODEM <modem #> of DM card in slot <slot #> is unusable
An attempt was made to perform an operation on a specific modem that had been deleted from the usable list via the *modem delete* command. Use the `modem add` command to make the modem usable again, or use a different modem to perform the desired operation.

MODEM CONNECT failed - connect <connect id #>, board <board #>, modem <modem #>
An attempted modem call has failed to connect. Try reconnecting the call again. If this message consistently appears for the same modem number, contact your distributor or Customer Support.

Modem revision on modem <modem #> of slot <slot #> failed
Individual modems on a Digital Modem card are failing. Check the hardware and software configurations, as well as the seating of the card and the MVIP cabling. If all seems in order, contact your Distributor or Customer Support.

Negotiation Failure with Semipermanent device "x"
There was some problem negotiating a connection with device "x." There was no way to send data. This could be an authentication failure or a PPP failure.

Network loop between site1 and site 2
The system detected a WAN loop between the specified sites, so the System will not forward the duplicate frame. Check the System and network configuration for this loop and adjust.

Network requested init but no SPID configured- Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
A SPID is required but is not configured on the indicated line. The configuration of the SmartSwitch Remote Access Module or of the switch should be corrected.

Network sent bad Endpoint identifier - Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
During terminal initialization, a bad endpoint identifier was received on the indicated line. This message is informational only; your line should continue to operate normally.

Network sent CAUSE - invalid SPID - Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
An invalid SPID is configured on the indicated line. The configuration of the SmartSwitch Remote Access Module or of the switch should be corrected.

Network sent Cause - SPID not supported - <slot #, port #>
The indicated line does not support SPIDs; however, a SPID is configured for use on the line. Is the SPID configured incorrectly? Do you have the right switch type? Check the configuration. If the message persists, contact your BRI provider to determine corrective action.

Network sent STATUS with state = 0, tear down call
A STATUS message has been received from the network indicating that a specified call is not active. The system is removing the call.

No Active Calls
0 Active Sites
Currently, no sites are connected to the system.

No Active List entry available in INM
The system tried to contact a remote site and no table entries were available. You may need a larger version of the SmartSwitch Remote Access Module.

No CCB found, Port=<port #>, CallRef=<call reference #>
Contact your Distributor or Customer Support. Provide your distributor with a copy of the message log, and the output of the `wan stats` command. With the `wan stats` command, the main item of interest is the "rcv fail" number on the connections line.

No compression sessions are available due to memory constraints.
Check available memory; upgrade to a 12Mb system (minimum). If you are still encountering problems, disable unused protocols, and / or contact your Distributor or Customer Support to reduce your number of available connections.

NO FR LMI transmit buffer available
Indicates that, temporarily, no transmit buffer was available for formatting and sending a STATUS ENQUIRY message to the network.

NO FR LMI transmit buffer descriptor available
Indicates that, temporarily, no transmit buffer descriptor was available for control and administration of a STATUS ENQUIRY message to be sent to the network.

No internal b channel resources available, disconnecting call
The call is up, but there are no resources available to send the data. Contact your Distributor or Customer Support.

No resources available to accept incoming call
The System received an incoming call, but it had already established the maximum number of calls. This indicates the demand for network resources exceeds the configuration of this system. If this type of occurrence continues, you should consider upgrading to a larger system.

No response to TEI requests - Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
TEI configuration mismatch between the system and the switch for the indicated line. The configuration of the system or of the switch should be corrected.

No Sites Connected
Currently, no sites are connected to the system.

Not enough memory for Security module
Not enough system memory available to operate security module. Contact your Distributor or Customer Support.

No UA seen in response to SABMEs - Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
Layer 2 cannot be established between the system and the switch. This could be a TEI configuration mismatch between the system and the switch for the indicated line. Check the configuration of the system. If this is not the problem, call your carrier. The configuration of the switch may need correction, or the line may need to be manually restarted.

No VCB buffer available
Ran out of sending buffers for messages to Combinet. If this is a recurring problem, contact your Distributor or Customer Support.

Number of optional connections reduced from xx to yy due to memory limitations
This informational message identifies that there is not enough memory available to accommodate the system's total capacity load for optional connections.

Number of required connections reduced from xx to yy due to memory limitations
This informational message identifies that there is not enough memory available to accommodate the system's total capacity load for required connections.

Offnode server lookup of Dial Out User failed.
Off-node authentication was not successful. Most likely, the device attempting to authenticate was not configured. Check configuration.

OSW <OSWFileName>, found in the Flash File System. The OSW has not been updated from this file due to insufficient Flash File System space. Please delete unnecessary files from the system.
Delete unneeded files to free up Flash File System space, and reboot the system. DO NOT DELETE NEX.BIN, IOP.BIN, OR UPGRADE.BIN. The system will again attempt to install the compressed file set after the system is rebooted again.

Outgoing calls barred - Slot=<slot #> Port=<port #>
The system cannot place outgoing calls on the indicated line. The switch must be configured to handle circuit switched data calls. Contact your phone company and report the problem.

Out of CCBs, Port=<port #>, CallRef=<call reference #>
Contact your Distributor or Customer Support.

Out of LAN Adapter transmit command descriptors
The LAN adapter is temporarily out of buffers used to transmit frames on to the Ethernet. This condition should clear. If it persists, contact your Distributor or Customer Support.

Out of overflow RAM buffers
Contact your Distributor or Customer Support.

Out Svc # <slot #, port #>
ISDN line failure. The line connected to the indicated slot and port is out of service for the reason indicated by #.

1 = No layer 1 sync for 5 seconds
This problem normally occurs due to WAN cabling problems.
Check your cables to make sure they are connected correctly. If this problem still occurs after you have checked all the cables, call the phone company and report the problem.

2 = No response to TEI requests
This problem normally occurs due to invalid configuration.
Check your configuration using the following table:

basic rate	*line from phone co: point-to-point*	*line from phone co: multi-point*
line configured on non-auto TEI	make sure that the configured TEI value is 0	change TEI to be AUTO
line configured on auto TEI	change TEI to be non-auto	if problem happens for over 5 minutes, report problem to phone company

3 = No UA response to SABME requests; no Layer 2
This problem normally occurs due to invalid configuration.
Check your configuration using the previous table.

4 = Failure to negotiate SPID (U.S. only). This is due to an improperly configured SPID. Check your configuration.

5 = Failure to negotiate SPID (U.S. only). SPID has not been configured on the system; check configuration.

Over Max Charge
Monthly call charges exceeded. Monthly call charge tracking is enabled and the configured maximum has been exceeded.

[PAP] Identification timeout on remote device
The remote device did not send the PAP Authenticate-Request packet within a required amount of time. Try again. If this persists, contact your remote site.

[PAP] Invalid password for <name> given by remote device
The system received the PAP Authentication-Request packet with the incorrect password for the device name <name>.

[PAP] Remote device did not respond to the request
The system sent PAP Authenticate-Request packets the maximum number of times, but the remote device did not send either Authenticate-Ack or Authenticate-Nak packets. The remote device may not be working properly. Check the configuration of the remote device and reboot. If the problem recurs, contact your Distributor or Customer Support.

[PAP] Remote device rejected System Information <error message>
The system received the PAP Authenticate-Nak packet with the error message <error message> against the previous PAP Authenticate-Request sent by the system. The <error message> is from the remote device, and is device-specific. Contact the remote site for assistance.

[PAP] Unknown name <name> given by remote device
The system received the PAP Authenticate-Request packet with the unknown device name <name>.

Post <number>, HDLC #<number> External Loopback Test FAILED
The indicated HDLC controller, 80532 Device, failed an internal register test. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number>, HDLC #<number> Internal Loopback Test FAILED
The indicated HDLC controller, 80532 Device, failed an internal loopback test. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number>, HDLC #<number> Interrupt Test FAILED
The indicated HDLC controller, 80532 Device, failed an internal interrupt test. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number>, HDLC #<number> Register Test FAILED
The indicated HDLC controller, 80532 Device, failed an internal register test. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number>, HDLC #<number> Test FAILED
The indicated HDLC controller, 80532 Device, failed one of the constituent POSTs. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number>, ISDN Test FAILED
The specified D-channel controller, one of 4 2086 devices, did not pass its POST. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number> memory read error at <address>, expected <value>, read <value>
The specified memory POST failed at the specified address, with both the expected and actual memory values displayed. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number> NVRAM Failure
The non-volatile RAM failed during its POST. The boot process should continue; however, make note of the error message in the event of a future problem.

Post <number>, timed out waiting for i960 to respond during POSTs
The i960 failed to respond during the allotted amount of time during the specified POST. This is an i960 failure. The boot process should continue; however, make note of the error message in the event of a future problem.

[PPP] Link Failure Detected: No response to periodic Echo-Requests.
This message is logged by the feature when it detects a failed link.

PVC for DLCI <dlci index> not ACTIVE
A frame was received on the PVC associated with the indicated DLCI which was not active. This is a temporary condition, and results from an asynchronous operation between the network and customer-premise equipment regarding the state of the individual PVCs. If this problem persists, contact your Distributor or Customer Support.

PVC not allocated for <dlci index>
The frame relay software received a frame from the network on PVC using the indicated DLCI which has not yet been configured. It is likely that there is a configuration mismatch between nodes in the network such that a node is transmitting data to the node logging this error via a valid but as yet unallocated PVC.

PVC rcv wait q already full
Indicates a lack of system resources to handle the level of traffic being experienced. Contact your Distributor or Customer Support.

RADIUS authentication is not available. You must first ENABLE RADIUS user level authentication.
An attempt was made to configure the Terminal Server Security for RADIUS and RADIUS was not configured on the SmartSwitch Remote Access Module.

RBS: Channel <channel #> - Backing off of channel, GLARE detected.
An incoming and outgoing call occurred on the indicated channel at roughly the same time. The system discontinued the outgoing call in order to allow the incoming call to be established.

RBS: Encountered unknown source ID.
RBS_out_SM<channel #>: NO Dial Digits supplied.
RBS: Received unknown primitive from CC.
RBS: Received unknown primitive from L1.
RBS: Received unknown primitive from ME.
RBS: Received unknown primitive from RBS.
The above Robbed Bit Signaling messages indicate that the system software sent a message to the RBS state machine that the state machine was unable to recognize or the information was incorrect. If this message is displayed in the log messages, contact your Distributor or Customer Support.

RBS: LIF_AddTimer failure.
An event occurred that the RBS task interpreted as a call signaling event, but layer 1 is not properly initialized. Ensure that an ISDN line is not plugged into a RBS card.

RBS: LIF_GetBuffer failure.
RBS: Unable to send host CALL_CLEARED.
RBS: Unable to send host CALL_CONNECTED.
RBS: Unable to send host CALL_REQUEST_ACK.
RBS: Unable to send host HOST_CALL_INDICATION.
RBS: Unable to send host REMOTE_DISCONNECT
RBS: Unable to send package to host.
The above Robbed Bit Signaling messages indicate that the WAN card is not communicating properly with the host, probably due to a card failure. Contact your Distributor or Customer Support.

RBS_out_SM<channel #>: Timeout waiting for WINK.
The system went off-hook and the switch never "winked" back, going off-hook for a specified amount of time and then returning to on-hook. The switch must wink back in order to tell the system to start dialing. Contact the telephone company and ensure that the line is configured for wink-start.

RBS: Unexpected event chan = <channel #>, state = <state ID>
An illegal signaling event occurred in the RBS task on the specified channel. Ensure that the line is configured correctly and that it is using the expected RBS protocol. Excess noise on the line may also cause this event.

Read 0 bytes from file <file name> for WAN card in slot <slot #>
If seen repeatedly, the above message indicates a problem with your hard drive. Contact your Distributor or Customer Support.

Ready for XModem Download - <ESC> to abort
The user has requested an attempt to UPDATE the system software, or it was not possible to Boot the system the last time it was attempted.

Reattempting to Install File Set into Flash Memory
The SSB is re-attempting to install the FileSet. The Flash File System may have been corrupted when attempting to install the FileSet the first time. In the meantime, the Flash File System has been formatted.

Rebooting...
The system is going to wait until the WatchDog timer expires, which causes the entire system to reboot.

Received charge amount - <charge amount>
The system has received an advice of charge from the network for the call just disconnected. The charge for this call is indicated in the charge amount parameter.

Received CLLM while PVC for DLCI <dlci index> in unexpected state <state>
A CLLM message was received indicating that a network condition should be expected for the PVC associated with the indicated DLCI. However, this PVC is in the indicated state and as such is already acting on a previous network condition notification.

Remote peer ID discrepancy
The On-node Device Table and the remote end of the connection disagree on the identity of the remote end. Check configuration, and then reboot the remote device. If problem persists, contact your Distributor or Customer Support.

Replace Lithium Battery: Contact your Representative
If this message is displayed in the log messages, contact your Distributor or Customer Support before you power off your system.

Requested channel not available - <slot #, port #>
The system has attempted a call using a channel on the indicated line that was not available. The call will be retried over a different line if possible.

Reserved signal
This message is informational only and is used to indicate additional details on the <signal value> received in the "call progress" information message.

Resmem_gettotal: Enabled size <size>, greater than Checksize <size> for <sub name>
Internal error that should be reported to Customer Support.

ResMem_Malloc failure for subsystem <sub name>
(size=<size>, type=<type>, class=<class>, ra=<hex return address>)
ResMem_Malloc Size <size> too large for subsystem <sub name> (type=<type>, class=<class>
ra=<hex return address>)
ResMem_Malloc Device not registered (ra=<hex return address>)
ResMem_Obtainable Device not registered (ra=<hex return address>)
Any of the above three messages indicate that an internal error has occurred that should be reported to Customer Support. The system will restart when this error occurs.

Retrying download of DM card in slot <slot#> in <x> seconds
The system has failed on previous attempts to initialize the Digital Modem card. The system will retry a specific number of times before logging a failure message. Check the hardware and software configuration, reseat the card in its ISA slot, and / or check the MVIP cabling. If the problem persists, contact your Distributor or Customer Support.

Rx Channel Inactivity Detected
No keep-alive frames have been received over an active connection to a remote system. This indicates that the connection or the remote node has failed (or been powered-off) without an indication of the failure from the network. If the event continues, contact your Distributor or Customer Support.

Security Rejection - Bridge Address Security cannot use Authentication Server
Both options (Bridge Address Security and off-node User Authentication) are not supported simultaneously.

Security Rejection - Caller did not negotiate security
Bridge Security is configured. A caller attempted to send device data before (or without) negotiating the Bridge Address security.

Security Rejection - HDLC not supported by the caller
A properly formed Bridge Security negotiation packet was received but the remote bridge indicated that it did not support the HDLC protocol.

Security Rejection - Invalid Calling Line Id - <CLID>
The calling line identifier has not been configured for any valid device in the system Device list. The number <CLID> indicates the actual number presented by the network.

Security Rejection - Invalid Password (<password>) given
A properly formed Bridge Security negotiation packet was received. The bridge is registered in the System Device table and a password was provided, but the password provided did not match the password in the System Device table.

Security Rejection - No Bridge Address given by caller
A normal Bridge Security negotiation packet was received, but did not contain a bridge address. Check configuration. If problem persists, contact your Distributor or Customer Support.

Security Rejection - No Password given by caller
A properly formed Bridge Security negotiation packet was received, and the bridge is registered in the system, but a password is required and none was provided by the calling bridge. Check configuration. If problem persists, contact your Distributor or Customer Support.

Security Rejection - No Protocol List supplied
A Combinet has attempted to connect to the system without the required Protocol List information. Check configuration, and then reboot the Combinet. If problem persists, contact your Distributor or Customer Support.

Security Rejection - Timeout on Startup Complete
After a normal Bridge Security negotiation packet is received, and the System sends a response message, there is a five second time limit in which a “Startup Complete” message must be received. The above security rejection message is seen if the Startup Complete message is not received before the timer expires. Check to see if the response message was received by the calling bridge.

Security Rejection - Unknown Calling Bridge - <bridge address>
A properly formed Bridge Security negotiation packet was received but the bridge address is not registered in the system.

SemiPermanent. Local authentication failure of Semipermanent device "x"
The system failed to authenticate the indicated device. The semipermanent connection will be disabled. Compare the authentication device information configured on the system with the actual configuration of the remote device. Make corrections as needed. Then, issue the `call device <device name>` command to reinstate the semipermanent connection.

Semipermanent. Device "x" disconnected by admin
The administrator has issued a `disc device <device name>` command. Therefore, the system will not attempt to call the indicated device again. Issuing the `call device <device name>` command will make device "x" semipermanent again.

Semipermanent. Device "x" has a smaller Initial Data Rate than Base Data Rate. No connection made.
The semipermanent feature will make enough calls to meet but not exceed the device's Initial Data Rate. In this case, the Base Data Rate (normally 56 or 64 Kbps) is larger than the device's Initial Data Rate. The semipermanent feature cannot make any calls, or it will exceed the Initial Data Rate. Reconfigure your data rates.

Semipermanent. Device "x" has had "y" bandwidth drops within "z" seconds. This device is considered to have failed remote authentication.
Because the local system cannot always be aware of remote authentication failures, and because there is no way to recognize remote authentication failures in the system once the remote end is authenticated, the semipermanent feature will try to determine them by detecting excessive remote bandwidth drops. The remote device must drop a call 10 times within a 10 minute period to trigger this event.

> *Will try again in "w" minutes.*
> This will be displayed directly beneath the above message if a Session Interval is configured for the device.

Semipermanent. Device "x" reconnected by admin.
The administrator has issued the `call device <device name>` command after issuing the `disc device <device name>` command. This restarts the semipermanent feature for the indicated device.

Severe congestion CLLM received for DLCI <dlci index>
A CLLM message was received indicating severe congestion may be expected on the PVC associated with the indicated DLCI.

Signal for unknown CallCmd task: <task Id>
Contact your Distributor or Customer Support.

<slot #, port #> Cfg Error
Line vs. adapter configuration error. A line is configured for port <port #> that does not exist on the adapter in slot <slot #>.

[SNMP] Authentication failure, improper access rights
There are two possible causes for this message:

- The SNMP Agent received a SetRequest PDU that contained a Community Name with an MIB access level of MIB GUEST or MIB USER. The MIB access level must be MIB ADMIN to perform a SetRequest. The request was discarded.
- The SNMP Agent received a PDU that contained a Community Name with an MIB access level of MIB GUEST and an object Id that cannot be accessed with an MIB GUEST access level. The request was discarded.

[SNMP] Authentication failure, unknown community name
The SNMP Agent received a request PDU whose community name is not configured. The request was discarded.

[SNMP] SNMP initialization failure - unable to allocate necessary memory
The SNMP feature was unable to initialize because it could not obtain the necessary memory. The SNMP feature is disabled and no SNMP request will be processed. Contact your Distributor or Customer Support.

[SNMP] SNMP initialization failure - unable to open UDP port
The SNMP feature was unable to initialize because it could not obtain the necessary UDP port. The SNMP feature is disabled and no SNMP request will be processed. Check the configuration, and then contact your Distributor or Customer Support.

[SNMP] SNMP initialized successfully
The SNMP Agent has been successfully initialized and is fully operational.

[SNMP] Unable to obtain an SNMP Trap queue entry buffer
The SNMP Agent attempted to generate a TRAP PDU but was unsuccessful because it could not obtain necessary memory. The TRAP was not sent. Contact your Distributor or Customer Support.

[SNMP] Unable to obtain an SNMP Trap queue header
The SNMP Agent attempted to generate a TRAP PDU but was unsuccessful because it could not obtain necessary memory. The TRAP was not sent. Contact your Distributor or Customer Support.

SPID FSM got unidentifiable INFO msg - Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
An unexpected information message was received from the network on the indicated line. If you are having trouble establishing calls on this line, the problem should be reported to your phone company.

SSB: Can't read RTC prior to i960 POSTs
The Real Time Clock became inaccessible before invoking the i960 POSTs. The RTC is used to guard against infinite loops while waiting for the i960 to run its POST tests. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Couldn't read RTC during i960 POSTs
The Real Time Clock became inaccessible during the running of the i960 POSTs. The RTC is used to guard against infinite loops while waiting for the i960 to run its POST tests. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: i960 I/O memory copy differs from flash image at <address>
After loading the i960 POST tests into the I/O memory, a value unexpectedly changed at the address given.

SSB: i960 Memory read error at <address>, expected <value>, read <value>
While testing the shared memory area (I/O memory and the peripheral buffer memory), an error was detected. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: i960 POST number not equal to i386's
The i386 requested the i960 to run a specific POST. Upon receiving the response, from the i960, it was determined that a different POST was actually run.
The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 23 i960host_int_reg FAILURE
The i960 failed its internal register test. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 24 i960io_int_reg FAILURE
The i960 failed its I/O register test. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 25 i960io_mod_mem_1 FAILURE
The i960 failed its I/O memory test using the first test pattern. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 26 i960io_mod_mem_2 FAILURE
The i960 failed its I/O memory test using the second test pattern. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 27 i960timer_82c54FAILURE
The i960 failed its timer unit test. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 28 i960lan_82596sx FAILURE
The i960 failed its LAN Coprocessor test. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 29 i960lan_82503 FAILURE
The i960 failed its LAN transceiver test. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 30 i960per_mod_mem_1 FAILURE
The i960 failed its peripheral buffer memory test using the first test pattern. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 31 i960per_mod_mem_2 FAILURE
The i960 failed its peripheral buffer memory test using the second test pattern. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 32 i960hdlc_1 FAILURE
The i960 failed its 80532 test using the first HDLC controller. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 33 i960hdlc_2 FAILURE
The i960 failed its 80532 test using the second HDLC controller. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 34 i960hdlc_3 FAILURE
The i960 failed its 80532 test using the third HDLC controller. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 35 i960hdlc_4 FAILURE
The i960 failed its 80532 test using the fourth HDLC controller. The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Post 36 i960isdn_1 FAILURE
SSB: Post 37 i960isdn_2 FAILURE
SSB: Post 38 i960isdn_3 FAILURE
SSB: Post 39 i960isdn_4 FAILURE
The i960 failed its 2086 test using the first (second, third or fourth) D-channel controller The boot process should continue; however, make note of the error message in the event of a future problem.

SSB: Timed out waiting for i960 to initialize for POSTSs
The i960 did not respond to an initialization request in a timely manner. This is a i960 failure. The boot process should continue; however, make note of the error message in the event of a future problem.

Starting Triggered RIP/SAP for <device>
This message indicates that triggered RIP / SAP has started for a device (either locally configured or one present in the WAN peer list). Triggered RIP / SAP has been configured as a routing protocol for this particular device.

Stream Ready rejected - MTU too small
The remote device will only accept the stream connection if the MTU is set to be $\geq$ 1514. Check to make sure that the remote device and the SmartSwitch Remote Access Module MTU value is set to $\geq$ 1514.

[STP] A BLAN Topology Change has been detected
The system has detected a topology change in the Spanning Tree environment.

[STP] A new Root Bridge has been detected
The system has detected a new root bridge for the Spanning Tree environment.

[STP] LAN Port <port #> is now a Designated Port
The indicated LAN port has become the designated port for the attached LAN.

[STP] LAN Port <port #> is now the Root Port
The indicated LAN port has become the root port for the system.

[STP] This Bridge is now the Root Bridge
The system has become the root bridge for the Spanning Tree environment.

Successfully Loaded Release <X.Y> Issue <Z>
The specified release of System software was successfully loaded into memory.

Switch could not recognize phone number nnnnnnn
The switch did not accept the phone number dialed as a complete number. Check the correctness of the phone number (including any leading digits such as 8 or 9).

System Clock Fault on Wan Adapter in Slot <slot #>
Indicates a TDM bus connection failure. Check to make sure that the TDM bus has been correctly connected.

TACACS authentication is not available. You must first ENABLE TACACS user level authentication.
An attempt was made to configure the Terminal Server Security for TACACS and TACACS was not configured on the SmartSwitch Remote Access Module.

TCP Connection to VRA Manager Lost
The TCP connection to the SFVRA Connection Manager has gone down.

TDM Clock Master changed TO (slot #, port#) FROM (slot #, port #)
The Clock Manager has dynamically adjusted the master clock source in response to an external line state change.

Temporarily unable to read flash file system due to flash reclaim in progress - try again later
The system is automatically performing a flash reclaim to reclaim space previously occupied by deleted files. Wait several seconds (up to a minute maximum) and try your file system command again.

Terminal Server Security connections disabled. Dropping call.
The Terminal Server Security is set to *none* and a terminal connection was requested. Check configuration. Most likely, the Default Async Protocol is set to terminal with no Terminal Server Security configured.

Terminal Server Security is currently using this database. You must change the Terminal Server Security setting first.
An attempt was made to disable a User Level Security Database when the terminal server was configured to use this database for terminal mode authentication.

[TFTP] Data buffer allocated successfully
All parts of the TFTP feature (both Server and Client) were successfully initialized.

Note: The following "[TFTP] Local error..." messages generated during client operations will be displayed on the console only and will not be logged to disk.

[TFTP] Local error #2: Feature not initialized
The TFTP feature was not initialized properly. No file transfer will be attempted. Check the configuration, and then contact your Distributor or Customer Support.

[TFTP] Local error #3: Server not initialized
The TFTP Server was not initialized. The TFTP Server will not attempt any file transfers. Check the configuration, and then contact your Distributor or Customer Support.

[TFTP] Local error #4: UDP rejected packet <filename>
The UDP subsystem could not send the data because there was a problem with the file. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #5: UDP open failed
The UDP subsystem could not open a new port. No file transfer will be attempted. Check the configuration, and then contact your Distributor or Customer Support.

[TFTP] Local error #6: All UDP buffers in use <filename>
All of the TFTP / UDP buffers are in use. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #7: Received packet with size zero
The TFTP protocol received a packet with no data.

[TFTP] Local error #8: No route defined <filename>
The TFTP protocol was instructed to start a TFTP session with an IP ADDRESS (HOST) for which there is no defined route. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #9: File transfer timed out <filename>
The TFTP file transfer timed out. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #10: IP addressing inconsistency detected
The TFTP protocol received a packet from a host for which no file transfer was being processed. This should not affect any files being transferred.

[TFTP] Local error #11: Received packets out of sequence <filename>
The TFTP protocol received a data packet that either was too old or one was skipped. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #12: Bad packet length received <filename>
The TFTP protocol received a packet that was too big. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #13: Received unexpected opcode <filename>
The TFTP protocol received a packet that was not expected. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #14: Bad file name
The local file (as defined from a remote host) was not recognized as a valid file name. No file transfer will be attempted.

[TFTP] Local error #15: Bad mode string
The TFTP mode string was not NETASCII nor OCTET. No file transfer will be attempted.

[TFTP] Local error #17: Unable to locate file/directory <filename>
The file system was unable to locate the file requested. No file transfer will be attempted.

[TFTP] Local error #18: Unable to open file <filename>
Either the file does not exist or the device (Client or Server) does not currently have access to this file. No file transfer will be attempted.

[TFTP] Local error #19: Disk full <filename>
The local disk became full during the TFTP file transfer. There may be a problem with the specified file; try replacing it. If this message appears consistently, contact your Distributor or Customer Support.

[TFTP] Local error #20: Error while writing file <filename>
An error occurred while writing to a file. The file may be corrupted and must be replaced.

[TFTP] Local warning #21 All sessions in use
All of the allowed TFTP sessions are currently in use. No file transfer will be attempted. (TFTP client console message only; not logged on System.)

[TFTP] Local warning #26 TFTP Session Killed
The TFTP session was terminated by the network administrator via issuing the *TFTP kill <session Id>* console command.

Note: For the following [TFTP] Remote error messages the Remote Host TFTP Servers/Client will map error messages within the types shown below. The text portion of each message may vary with each Host transmitting the message.

[TFTP] Remote error #0: (Text from Remote Host)
Undefined error. The accompanying text (if any) should describe the error. The file being transferred may be corrupted.

[TFTP] Remote error #1: (Text from Remote Host)
The REMOTE HOST could not find the file specified on its system. No file transfer will be attempted.

[TFTP] Remote error #2: (Text from Remote Host)
The REMOTE HOST is reporting an access violation of the specified file. No file transfer will be attempted.

[TFTP] Remote error #3: (Text from Remote Host)
The REMOTE HOST is reporting that its disk is full. The file being transferred may be corrupted.

[TFTP] Remote error #4: (Text from Remote Host)
The REMOTE HOST is reporting that it received a TFTP packet that it was not expecting. The file being transferred may be corrupted.

[TFTP] Remote error #5: (Text from Remote Host)
The REMOTE HOST is reporting that it was not expecting a packet from our system. The file being transferred may be corrupted.

[TFTP] Remote error #6: (Text from Remote Host)
The REMOTE HOST is unable to overwrite the specified file. No file transfer will be attempted.

[TFTP] Remote error #7: (Text from Remote Host)
This message indicates that the specified device does not exist. This error should not occur since TFTP does not use Device Ids.

[TFTP} Server UDP port (69) closed successfully
Informational message stating that the TFTP server UDP port was successfully closed.

[TFTP} Server UDP port (69) opened successfully
Informational message stating that the TFTP server UDP port was successfully opened.

[TFTP] Unable to allocate data buffers
The entire TFTP feature (both Server and Client) was not initialized. Contact your Distributor or Customer Support.

[TFTP] Unable to open Server UDP port (69)
The TFTP Server was not initialized; however, the TFTP Client may still work. If this message occurs repeatedly, or if the TFTP Client does not work, contact your Distributor or Customer Support.

The call deflection selection is prior to CCITT 1988
Verify that the facilities provided by the service provider are CCITT 1988.

The call has been disconnected
A call has been up longer than the amount of time configured and has been taken down.

The call is allowed to continue
A call has been up longer than the amount of time configured, but it has not been taken down.

The compression subsystem is not enabled
Check SFVRA-CFG; verify that compression is enabled.

The conformance selection is prior to CCITT 1988
Verify that the facilities provided by the service provider are CCITT 1988.

The RADIAC Feature is no longer supported. The RADIAC feature has been replaced by the TACACS Feature. The TACACS Feature configuration must be completed before usage.
With the addition of User Level Security, the need for the RADIAC GATEWAY is gone. The SmartSwitch Remote Access Module has incorporated the functionality of the RADIAC GATEWAY within the SmartSwitch Remote Access Module itself. When the configuration file parser encounters a system configured for using the RADIAC feature, it switches the configuration to now use User Level Security utilizing a TACACS off-node authentication server. Since the older SmartSwitch Remote Access Module knew nothing about the location of the TACACS server, the TACACS server configuration must be completed before the SmartSwitch Remote Access Module will allow network access through a WAN connection.

Timeout detected on connection establishment
The system initiated a connection with a remote site, but a time-out occurred while waiting for a connection response from the network. Verify that the remote site is active and that the network is operational.

Timeout detected on receiving caller's number
The incoming call security feature is enabled and the caller's number was not received, so the call was disconnected. Contact your phone company and verify that your switch supports passing along the calling number information element. (This is sometimes referred to as ICLID for InComing Line Identification).

Timeout on SPID Exchange - Slot=<slot#> Port=<port #> Ces=<communication endpoint suffix>
SPID exchange was not completed in time (i.e., switch never responded to the SPID). Check switch configuration to make sure the correct SPID value has been entered.

Timeout on Startup Complete
A startup complete message was not return from the Combinet after we sent the response a number of times. Check the configuration, and then reboot the Combinet. If problem persists, contact your Distributor or Customer Support.

Timeout waiting for DL Config Response
Timeout waiting for DSL Config Response
Timeout waiting for Terminate DSL Response
The above messages indicate that an attempt has been made to dynamically update the Data Link configuration, but the system did not receive a response from a Basic Rate adapter for an earlier request. Restart the system and review the configuration for the adapter. If the problem persists, the indicated adapter card may be faulty. Contact your Distributor or Customer Support.

Tried to free unallocated buffer <sub name>, size=<size>
Internal error that should be reported to Customer Support.

Transmit rate increased to <transmit rate>: Access <access index>, DLCI <dlci index>
The effective transmit rate has been increased to the indicated rate for the indicated DLCI under the indicated access.

Transmit rate reduced to CIR <transmit rate>: Access <access index>, DLCI <dlci index>
The effective transmit rate has been limited to the Committed Information Rate which is the rate for the indicated DLCI under the indicated access.

Type mismatch of configured & installed adapter #'x'
Configuration mismatch between the indicated adapter and the resource that was configured. The system resource configuration should be corrected.

Unable to add dynamically-obtained device data into Device Table
The System authentication type is configured to obtain device information off-node. If such information cannot be stored internally due to a temporary resource shortage, the call is dropped.

Unable to allocate IPX spoofing memory. IPX spoofing is being performed in a degraded mode.
The memory required by the IPX spoofing feature could not be allocated. The IPX spoofing code will continue to run but it will run in a degraded mode. The default IPX spoofing options will always be used when a connection is down to a device.

Unable to allocate port structure for port <port name> with address <AppleTalk Address>
Contact your Distributor or Customer Support.

Unable to allocate unnumbered wan port for device <device name>
Contact your Distributor or Customer Support.

Unable to complete Bridge Dial Out call: Insufficient information configured for Dial Out Device
Verify that *Bridging* and *Make Calls for Bridge Data* are enabled at the device level.

Unable to communicate with encryption board
Try again. If the problem persists, you may have a faulty encryption board. Replace the board.

Unable to Decrypt Datagram
An incoming datagram could not be decrypted. Verify encryption parameters on both nodes.

Unable to dynamically determine incoming call usage: Call Released.
This message refers to an incoming analog call which is going through the digital modem. The digital modem has transferred the call to the AUD to determine type of call. The AUD did not recognize any PPP LCP frames to transfer to the PPP stack, nor did it recognize the four carriage returns it requires (within 5 seconds of connection) for remote analog console access.

If you are attempting remote analog console access, be sure to press the carriage return four times within 5 seconds of making the connection.

Unable to get Digital Modem resource to place call
A Digital Modem dial-out call was attempted, and the system was unable to open a resource to place the call. Using the `modem status` command, check to ensure that there are usable modems available. If there are, and the problem persists, contact your Distributor or Customer Support.

Unable to Identify a remote device
A device that was not identified by any active security measures (for example, PAP or CHAP) was rejected.

Unable to Identify a remote device - <calling line id
A device that was not identified by any active security measures (for example, PAP or CHAP) was rejected and is identified by its Calling Line Id.

Unable to Identify a remote device - no CLID
A device that was not identified by any active security measures (for example, PAP or CHAP) was rejected and the caller did not present a Calling Line Id.

Unable to identify the frame type <CCB: xxxx>
The frame type (raw HDLC, RFC 1294, or PPP) can not be identified and therefore the connection has been terminated. "CCB: xxxx" is included for your Distributor or Customer Support. The most likely causes for the problem are: malfunction of the remote device, or a faulty line. Begin by checking the configuration of the remote device, and then rebooting the device. If this does not solve the problem, contact your Distributor. He/she will help you determine whether or not the line is faulty.

Unable to locate device entry in on-node database for terminal session
A device matching the login id entered at the user level security prompt was not found in the on-node database, and SFVRA Connection Manager was not configured.

Unable to open \config\devdb.nei file
Disregard this message if you have not yet added at least one device to the system's on-node device table and saved the change. The configuration file, \config\devdb.nei, is created the first time the device table is saved. If the message continues, contact your Distributor or Customer Support.

Unable to open Modem Upgrade file
There may be a problem with the modem revision file. Contact your Distributor or Customer Support.

Unable to restore original ISRs for Interrupt <interrupt #>
Check hardware jumpers and switches on the DM card and reinstall. Verify that the DM card is properly configured in SFVRA-CFG. If the problem persists, contact your Distributor or Customer Support.

Unable to send device information request to SFVRA after a terminal authentication.
Unable to send to SFVRA Connection Manager. Verify proper configuration of SFVRA-CONN and Call Control options.

Unable to send DL Config Request
Unable to send DSL Config Request
Unable to send Terminate DSL Request
The above three messages indicate that an attempt has been made to dynamically update the Data Link configuration, but the system is unable to send an update message down to a Basic Rate adapter. Restart the system and review the configuration for the adapter. If the problem persists, the indicated adapter card may be faulty. Contact your Distributor or Customer Support.

Unexpected error during transmission of LMI frame
A system error occurred during the actual transmit request for an LMI frame. Contact your Distributor or Customer Support.

Unknown Calling Bridge <MAC address>
MAC address security is enabled and the remote Combinet does not match any of the defined devices.

Unknown DLCI <dlci index> in CLLM message
The network has sent a CLLM message which has referenced the indicated DLCI that has not been configured. Check the system configuration for the indicated DLCI.

Unknown Security Association
An incoming datagram specifies a Security Parameter Index (SPI) which has not been defined on this node. Verify the encryption parameters on both nodes. Adjust if necessary so that both nodes reflect the same SPI.

Unmatched Login Task
This represents an internal system error. Contact your Distributor or Customer Support.

Unsupported Combinet protocol received: <protocol Id>
An unsupported Combinet protocol attempted to connect to the system. Contact your Distributor. You may need to upgrade software to support this.

Unsupported Combinet protocol version received: '<version Id>'. [Device: <device name>]
An unsupported Combinet version attempted to connect to the system. Contact your Distributor. You may need to upgrade software to support this.

Updating SmartSwitch Remote Access Module from "<FileName>"
The specified file, received during a Reliable Remote Upgrade, was successfully loaded into memory and will now be verified before installation into the Flash File System.

User Level Authentication flag is enabled for Terminal User xxx. Setting flag to disabled.

The device definition for xxx should have User Level Authentication disabled.
These two messages are displayed together. In device entries for terminal server connections, user-level authentication should not be enabled. In the event the SmartSwitch Remote Access Module finds an enabled condition, it will disable the pertinent flag for the duration of the call only. To avoid this situation permanently, disable the user level authentication flag in device entries for all terminal server connections.

Waiting for WAN card in slot <slot #> to complete initialization
Download process update for WAN card in slot <slot #>.

WAN card in slot <slot #> signals it is operational
Download process update that indicates that WAN card in slot <slot #> is now operational.

WAN Port is now in the Forwarding state
WAN port connections used by the bridge are now entering the specified state.

WAN Port is now in the <new state> state
The WAN connection port used by the bridge is entering the specified new state.

WAN: RBS Not Available on this card.
A RBS debugging command was attempted on a PRI card that is not configured for RBS. Check the card configuration and ensure you have the proper type of card.

Watchdog timeout detected on DM board in slot <slot #>
The Digital Modem card in the specified slot is not functioning properly. Check the board's configuration in SFVRA-CFG, reseat the board in its ISA slot, and check any MVIP bus cabling. If everything seems in order and the problem persists, contact your Distributor or Customer Support.

Watchdog timeout detected on WAN board 'x'
The system has detected that the indicated adapter has failed. This is a fatal condition and will cause the card to be reset. Verify the settings on the adapter. If theses are all correct and the problem persists, the indicated adapter card may be faulty. Contact your Distributor or Customer Support.

The following messages are reported when a remote X.25 device's facilities do not match with those configured locally:

X25 facilities error, facilities not allowed in PVC
A facility is configured, for example call deflection, which is not allowed in a PVC. Check your PVC configuration.

X25 facilities error, fast select with restriction on response was required
The fast select with restriction on response is required. Verify that fast select is enabled by both DTE's and the service provider.

X25 facilities error, bad facility length
The facilities length is missing. Contact your Distributor or Customer Support.

X25 facilities error, invalid facilities length
The length of the facilities packet is invalid. Contact your Distributor or Customer Support.

X25 facilities error, invalid DTE address
The supplied address in a X.25 call packet was invalid. Verify that the local DTE address configuration matches the address supplied by the service provider.

X25 facilities error, facility not allowed
A facility was requested which is not enabled. Verify that the specific facility is enabled by both DTE's and the service provider.

X25 facilities error, facility length too short
The length of the facilities packet is too short. Contact your Distributor or Customer Support.

X25 facilities error, invalid facilities parameter
A value was chosen for facility which is out of the acceptable range of values for that facility. The range of acceptable values for that facility should be verified at both DTE's and by the service provider.

X25 facilities error, reverse charging not allowed
The reverse charging facility was selected by the DTE. Verify that reverse charging is enabled by both DTE's and the service provider.

X25 facilities error, reverse charging not accepted
The reverse charging facility was selected by the DTE. Verify that reverse charging is enabled by both DTE's and the service provider.

X25 facilities error, fast select not available
The fast select facility was selected by the DTE. Verify that fast select is enabled by both DTE's and the service provider.

X25 facilities error, fast select not accepted
The fast select facility was selected by the DTE. Verify that fast select is enabled by both DTE's and the service provider.

X25 facilities error, throughput negotiation not allowed
The DTE throughput class does not match the throughput class available at either the DCE or the remote DTE, and throughput negotiation is not enabled. You should enable throughput negotiation at both DTE's. If this is not possible, or does not work, select the same throughput class at both DTE's.

X25 facilities error, closed device group not allowed
The closed device group facility was selected by the DTE. Verify that the closed device group facility is enabled by both DTE's and the service provider.

X25 facilities warning, reverse charging info not available
The service provider does provide reverse charging information. No action required.

X25 facilities error, facility not available
A facility was requested which is not enabled. Verify that the specific facility is enabled by both DTE's and the service provider.

X25 facilities error, packet length negotiation not allowed
The DTE packet length does not match the packet length available at either the DCE or the remote DTE, and packet length negotiation is not enabled. You should enable packet length negotiation at both DTE's. If this is not possible, or does not work, select the same packet length at both DTE's.

X25 facilities error, window size negotiation not available
The DTE window size does not match the window size available at either the DCE or the remote DTE, and window size negotiation is not enabled. You should enable window size negotiation at both DTE's. If this is not possible, or does not work, select the same window size at both DTE's.

X25 facilities error, RPOA not available
Recognized Private Operating Agency selection is not available. The System does not support this feature.

X25 facilities warning, transit delay not available
The service provider does provide transit delay information. No action required.

X25 facilities warning, charge inform not available
The service provider does provide charging information. No action required.

X25 facilities warning, call redirect notification not available
The service provider does provide call redirect information. No action required.

X25 facilities warning, NUI not available
Network device identification not available. No action required.

X25 permanent virtual circuit down: Access=<access index>, PVC=<PVC index>, LCN=<LCN>
The indicated X.25 virtual circuit is down. Switched backup connections will be used, if available. This message will occur if the other system is down, or if the network interface line is not connected, or if the authentication of the remote device failed.

X25 permanent virtual circuit to device <device name> up: Access=<access index>, PVC=<PVC index>, LCN=<LCN>
The indicated X.25 virtual circuit is operational.

XMODEM DATA FAILED CRC CHECKS
A file contained in the X-Modem file set has failed the CRC check. The system will automatically reset and attempt a reboot in an effort to correct the problem. If the system continues to fail, make note of the displayed messages, and call your distributor. A software update is likely needed.

Zone allocation failed, increase zone table capacity.
The number of AppleTalk zones has surpassed the configured zone table capacity. The SmartSwitch Remote Access Module configuration utility allows you to set the maximum number of defined and learned zone table entries. The default value is 512. The maximum is 2,000. You may need to reset the zone table capacity to a higher number.

Zone allocation failed, maximum capacity already configured
The maximum number of AppleTalk zones have been surpassed. Contact your Distributor or Customer Support.

TRACE MESSAGES

OVERVIEW

Trace messages include the following categories of messages:

1. Call Trace Messages
2. PPP Packet Trace Messages

Before trace messages can be logged to the system report log, you must first enable the type of trace you would like to use. Once enabled, the system includes the trace messages in the memory-resident report log. To access this log, use the following commands:

dr or *ds*	display reports or display statistics
er or *es*	erase current messages / statistics from memory
wr or *ws*	write reports / statistics to disk

When the system writes system messages to disk, it stores them in the following locations:

Directory:	`\log`
File Name:	`rprt_log.nn` (where "nn" is an integer that is incremented each time a new file is written.)

The system reports messages using the following format:

Message Type		Time	Report Number	Message
I	Informational	hour:minutes:second	internal ID for area reporting the message	actual text of the message
W	Warning			
E	Error			

Where:

- The Message Type quickly identifies the type of message the system reports.
- The Time identifies when the message was reported.
- The Report Number is used by your Distributor or Cabletron Customer Support.
- The Message text describes the actual message being reported.

Below, there is a separate section included for each category of trace messages. For each category, a definition of the trace message type, the command to enable / disable the logging of the trace messages, and an alphabetized list of the associated messages is included.

CALL TRACE MESSAGES

A feature of the SmartSwitch Remote Access Module console is the ability to save and display a record of the high level ISDN calls between the system and the local telephone switch. If calls are unable to be completed, this is normally the first area to look.

Call Trace puts messages into the Report log that can be read by using the *dr* command. Call Trace is enabled by using the *trace on* command, and disabled by *trace off*.

The following is a description of the possible fields included in a Call Trace Message:

1. The <Call Id> field in the message can be used to keep track of messages for the same phone call. This is useful when a system is making more than one call at a time.

2. The In-Disconnect and In-Information messages have a location field. This identifies where the message originated.

   The following chart provides a list of locations that may appear in Call Trace messages:

Location Causes	
Value	*Meaning*
0	remote device
1	private local network
2	public local network
3	transit network
4	private remote network
5	public remote network
7	international network
FF	local SmartSwitch Remote Access Module system

3. The In-Disconnect messages have a cause field. This is the value (in hex) that was in the message. It explains why either a call was disconnected or why a call attempt was not able to be completed. There are also parameters (such as <signal value>, <progress value>), that are not described here. These values represent messages reported from the switch. We have attempted to interpret their significance in the error message text itself.

   Refer to the *Cause Codes* table, for a complete listing of cause codes.

When the call trace option is enabled, the system may report messages such as:

```
(I)    13:55:46.98 #1067: Out - CALL RQST CallId=0x8000 Rate=64 Slot=1 Port=1
       Chans=0x2 TN=181 Ces=0 ConnId=0
(I)    13:55:46.98 #1063: In - CALL RQST ACK CallId=0x8000 Slot=1 Port=1
       Ces=1ConnId=0
(I)    13:55:47.43 #1063: In - PROCEEDING CallId=0x8000 Slot=1 Port=1 Chans=0x1
       Ces=1 ConnId=0
(I)    13:55:47.60 #1063: In - CONNECT Call_id=0x8000 Slot=1 Port=1 Chans=0x0
       Ces=1 ConnId=0
(I)    13:55:54.16 #4D11: LAN Port 1 is now in the FORWARDING state
```

CALL TRACE MESSAGE SUMMARY

Access information discarded cause
Call trace message. This message is used to indicate additional details on the <cause value> received in the “call progress” information message.

Alerting off
Informational call trace message. The alerting signal information element is off. This indicates additional details on the <signal value> received in the “call progress” information message.

Alerting on - pattern <pattern number>
Informational call trace message. This indicates additional details on the <signal value> received in the "call progress" information message.

Answer tone on
Informational call trace message. This message is used to indicate additional details on the <signal value> received in the "call progress" information message.

Call has returned to the ISDN
Informational call trace message.

Call is not end-to-end ISDN
One or more of the WAN phone networks used to connect the call is not an ISDN network. The call must be at 56 Kbps.

Call waiting tone on
Informational call trace message. It indicates additional details on the <signal value> received in the "call progress" information message.

Custom tone on
Informational call trace message.

Delay in response at called interface
Informational call trace message.

Destination call address is non-ISDN
Informational call trace message.

Dial tone on
Informational call trace message.

Disconnect for <tone value> tone on
This message indicates that the system disconnected the outbound call. The <tone value> values are: error tone, busy verify, confirm, busy, network congestion, or intercept. These tone values indicate a temporary network failure. Check the outbound phone number and try again. If the problem persists, contact your phone company.

Expensive routing tone on
Informational call trace message.

In - ABNORMAL RPT Call Id=<call Id> Slot=<slot #> Port=<port #> ConnId=<connect Id> Ces=<communication endpoint suffix>
The system has detected an internal error condition. The <parameters> are included for your Distributor or Cabletron Customer Support. An error message describing the problem should be reported following this trace message.

In - ABNORMAL RSP Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix> Err=<error> Sev=<severity> State=<state>
The system has detected an invalid internal message type. Contact your Distributor or Cabletron Customer Support. The <parameters> are included for your Distributor or Customer Support.

In - ALERTING Call Id=<call Id> Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix> ConnId=<connect Id> Chans=<bearer channel map>
Informational call trace message. The system has received an alerting message from the network. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

Inband treatment has been applied
Call trace message (informational only). There are audible tones on the B-channel. (Refer to "Disconnect for <tone value>" message for possible tone values.) If the message persists, contact your Distributor or Cabletron Customer Support.

In -BRD CFG ACK Slot=<slot #>
This is an initialization acknowledgment message for the indicated adapter. It is in response to a configure message.

In - CALL RQST ACK Call Id=<call Id> Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix> ConnId=<connect Id>
A call request acknowledgment for the indicated call request.

In - CHAN STATUS Call Id=<call Id> Slot=<slot #> Port=<port #> Channel=<channel> Action=<action> ChanState=<channel state> SvcsState=<service state>
The system has received a channel status message from the network. This message is received when the status of a bearer channel on a line has changed. The <parameters> specify the channel and the new state.

In - CLEAR Call Id=<call Id> Slot=<slot #> Port=<port #> Loc=<location> Cause=<cause value> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system has received a call clear message from the network. This is usually received after a call disconnect is either initiated by the system or the network. The <parameters> are included for your Distributor or Cabletron Customer Support.Refer to the *Cause Codes Table* for more information.

In - configure ack <slot #>
This is an initialization acknowledgment message for the indicated line adapter. It is in response to a configure message.

In - CONNECT Call Id=<call Id> Slot=<slot#> Port=<port #> Chans=<bearer channel map> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system has received a connect message from the network. This indicates that a new call is now established and ready for use. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

In - DISCONNECT Call Id=<call Id> Slot=<slot #> Port=<port #> Loc=<location> Cause=<cause value> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system has received a disconnect message from the network. The Call Id and Ces values are for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details. Refer to the *Cause Codes Table* for more information.

In - DL CFG ACK Slot=<slot #> Port=< port #> Ces=<communication endpoint suffix
This is a data link initialization acknowledgment for the indicated data link.

In - DSL CFG ACK Slot=<slot #> Port=< port #>
This is a line initialization acknowledgment for the indicated line.

In - FACILITY ACK Call Id=<call Id> Slot=<slot #> Port=<port #> ConnId=<connect Id> Ces=<communication endpoint suffix>
The system has received a facility acknowledgment message from the network. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

In - FACILITY Call Id=<call Id> Slot=<slot #> Port=<port #> ConnId=<connect Id> Ces=<communication endpoint suffix>
The system has received a facility message from the network. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

In - FACILITY REJ Call Id=<call Id> Slot=<slot #> Port=<port #> Loc=<location> Cause=<cause> ConnId=<connect Id> Ces=<communication endpoint suffix>
The system has received a facility rejection message from the network. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details. Refer to the *Cause Codes Table* for more information.

In - INCOMING CALL Call Id=<call Id> Slot =<slot #> Port=<port #> Chans=<bearer channel map> Ces=<communication endpoint suffix> Rate=<data rate>
The system has received an incoming call from the network. The system will respond with a connect or a disconnect message. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

In - INFORMATION Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer channel map> CauseLoc=<cause location> Cause=<cause value> Signal=<signal value> ProgLoc=<progress location> Prog=<progress value> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system has received a call progress message from the network. This is usually received in response to sending a call request. The <parameters> are included for your Distributor or Cabletron Customer Support.Refer to the *Cause Codes Table* for more information.

In - init data link <slot #, port #, ces>
The WAN card in slot <slot#> attempted to initialize the data link for port <port#> with Communication Endpoint Suffix <ces>.

In - PROCEEDING Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer channel map> Ces=<communication endpoint suffix> ConnId=< connect Id>
The system has received a call proceeding message from the network. This is usually received in response to sending a call request. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

In - PROGRESS Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer channel map> CauseLoc=<cause location> Cause=<cause value> Signal=<signal value> ProgLoc=<progress location> Prog=<progress value> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system has received a call progress message from the network. This is usually received in response to sending a call request. The <parameters> are included for your Distributor or Cabletron Customer Support.Refer to the *Cause Codes Table* for more information.

In - REJECTION Call Id=<call Id> Slot=<slot #> Port=<port #> Loc=<location> Cause=<cause value> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system has received a call rejection message from the network. This is in response to sending a call request. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details. Refer to the *Cause Codes Table* for more information.

Interworking unspecified cause
Informational call trace message. This message is used to indicate additional details on the <cause value> received in the call progress information message. Refer to the *Cause Codes Table* for more information.

Off-hook warning tone on
Informational call trace message.

Origination call address is non-ISDN
Informational call trace message.

Out - ALERTING Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer channel map>
The system is sending a connection to the network. This is sent in response to receiving a call indication. The <parameters> are included for your Distributor or Cabletron Customer Support.

Out - BRD CFG Slot=<slot #>
The system is initializing the indicated adapter.

Out - CALL RQST ACK Call Id=<call Id> Rate=<data rate> Slot=<slot #> Port=<port #> Chans=<bearer channel map> TN=<telephone number dialed> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system is sending a call request to the network. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details.

Out - configure <port #>
The system is initializing the indicated line adapter.

Out - CONNECT Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer channel map> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system is sending a connection to the network. This is sent in response to receiving a call indication. The <parameters> are included for your Distributor or Cabletron Customer Support.

Out - DISCONNECT Call Id=<call Id> Slot=<slot #> Port=<port #> Cause=<cause value> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system is sending a disconnect to the network to terminate a call. The Call Id and Ces values are included for your Distributor or Cabletron Customer Support. The remaining parameters are used to report line details. Refer to the *Cause Codes Table* for more information.

Out - DL CFG Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
The system is initializing the indicated data link.

Out - DSL CFG Slot=<slot #> Port=<port #>
The system is initializing the indicated line.

Out - init data link <slot #, port #, ces>
The system is sending a message to the network to initialize a data link on an ISDN line. The <parameters> are used to report line details.

Out - PROCEEDING Call Id=<call Id> Slot=<slot #> Port=<port #> Chans=<bearer channel map> Ces=<communication endpoint suffix> ConnId=<connect Id>
The system is sending a connection to the network. This is sent in response to receiving a call indication. The <parameters> are included for your Distributor or Cabletron Customer Support.

Recall dial tone on
Informational call trace message.

Received charge amount - <charge amount>
The system has received an advice of charge from the network for the call just disconnected. The charge for this call is indicated in the charge amount parameter.

Received unknown abnormal report value Slot=<slot #> Port=<port #> Ces=<communication endpoint suffix>
Informational call trace message.

Received unknown progress value
Informational call trace message.

Received unknown signal value
Informational call trace message.

Ringback tone on
Informational call trace message.

Status report progress value received
Informational call trace message.

Stutter tone on
Informational call trace message.

Tones off
Informational call trace message.

Unspecified cause
Informational call trace message. This message is used to indicate additional details on the <cause value> received in the "call progress" information message.Refer to the *Cause Codes Table* for more information.

Unspecified tone
Informational call trace message. It is used to indicate additional details on the <signal value> received in the "call progress" information message. The <tone value> is displayed as one of the following: dial, ring back, answer, call waiting, off hook warning, custom, recall dial, stutter dial, or expensive routing.

PPP PACKET TRACE MESSAGES

PPP Packet Trace allows you to display the PPP protocol negotiation that takes place when a link is established. This information is useful when diagnosing mismatches in configuration between two systems. PPP Packet Trace puts PPP packet information into the Report log, which can be accessed by using the *dr* command. Enable this feature by using the *trace ppp on* command, and disable it with *trace ppp off.* Two other commands are also available, *trace ppp np* and *trace ppp cp*. *trace ppp np* only enables the tracing of Network Protocol packets received and sent by the system. When the *trace ppp np* command is used, no Control Protocol packets will be reported to the system message log. *trace ppp cp* only enables the tracing of Control Protocol packets received and sent by the system. When the *trace ppp cp* command is used, no Network Protocol packets will be reported to the system message log.

The following is the format of a PPP trace line as it is displayed by *dr:*
[connection Id] [packet direction] [protocol type] [packet type]

where:

[connection Id]
Identifies the connection. The Id is a numerical value, allowing you to distinguish connections. The numerical value represents the order in which the connections are generated.

[packet direction]
Indicates the packet direction. IN means received packet, OUT means transmitted packet.

[protocol type]
Indicates the type of protocol used for negotiation. When a connection is made between two devices, there are three different phases. The last two phases deal with the protocol type and the options negotiated.

The following table summarizes the protocol types:

Protocol	*Options Negotiated*
Link Control Protocol	Authentication Protocol (PAP,CHAP) Multilink Protocol (MRRU, Endpoint Discriminator)
PAP CHAP	Password validation Shared Secret validation
Compression (CCP) Encryption (ECP) IPCP BCP IPXCP ATCP	Compression options Encryption options IP address Bridge options IPX options Appletalk options

[packet type]
A code field that indicates the type of command that the packet contains. PPP Control Protocol negotiation uses the following commands:

- *Configure Request*
  The Configure Request is used to indicate the options that are supported by this sending device. The Request contains an option list and the desired values if they are different from the default value.

- *Configure ACK*
  The Configure ACK is transmitted in response to a Configure Request. It indicates that the sending device supports the options specified in the option list of the Configure Request and that all values are acceptable. The receiving device assumes that negotiation is complete for the Control protocol being configured.

- *Configure NAK*
  The Configure NAK is transmitted in response to a Configure Request. It indicates that the sending device understands, but does not accept the values of the options specified in the option list of the Configure NAK. The option list of the NAK only contains the unacceptable options. The receiving device should choose different options and send another Configure Request with the new option list and values.

- *Configure Reject*
  The Configure Reject is transmitted in response to a Configure Request. It indicates that the sending device does not understand the options specified in the option list of the Configure Reject. The option list of the Reject only contains the unknown options. The receiving device must assume the sender cannot process the rejected options in any manner, and take appropriate action. The Configure Reject inherently provides backward compatibility with older PPP implementations.

- *Terminate Request*
  The Terminate Request is transmitted when a device wishes to close down the connection.

- *Terminate ACK*
  The Terminate ACK is sent in response to a Terminate Request and indicates that the sending device has closed the connection.

- *Code Reject*
  The Code Reject is transmitted by a device if it does not recognize the PPP command type received from the other device.

- *Protocol Reject*
  The Protocol Reject is transmitted by a device if it does not recognize the PPP protocol type received from the other device.

- *Echo Request*
  The Echo request is used to provide a Data Link layer loop back detection mechanism. The Echo Request packet contains the magic number of the sending device. Until the magic number option has been negotiated the value must be set to zero.

- *Echo Reply*
  The Echo Reply is transmitted in response to an Echo Request. The Echo Reply packet contains the magic number of the sending device. Until the magic number option has been negotiated the value must be set to zero.

- *Discard Request*
  The Discard request packet is transmitted by a device to exercise the data link layer processing. This packet is silently discarded by the receiving device.

SYSTEM MAINTENANCE

This grouping of information provides information to help you maintain your SmartSwitch Remote Access Module once it is operating. Note that the included system statistics information may also prove valuable in troubleshooting.

We include the following chapters in the *System Maintenance* segment of the *User's Guide*:

- *Remote Management*
  Once the SmartSwitch Remote Access Module is initially configured, you may use methods to remotely manage the SmartSwitch Remote Access Module. This chapter provides information for using each of these methods.

- *System Commands*
  A listing of all system console commands and associated command definitions.

- *System Statistics*
  A listing of all system statistics and associated statistic definitions.

- *Routine Maintenance*
  Instructions for performing routing SmartSwitch Remote Access Module maintenance.

REMOTE MANAGEMENT

OVERVIEW

Once your system is initially configured (and thus assigned an IP address), you may use a variety of methods to remotely access and manage your system. This chapter describes many of these methods.

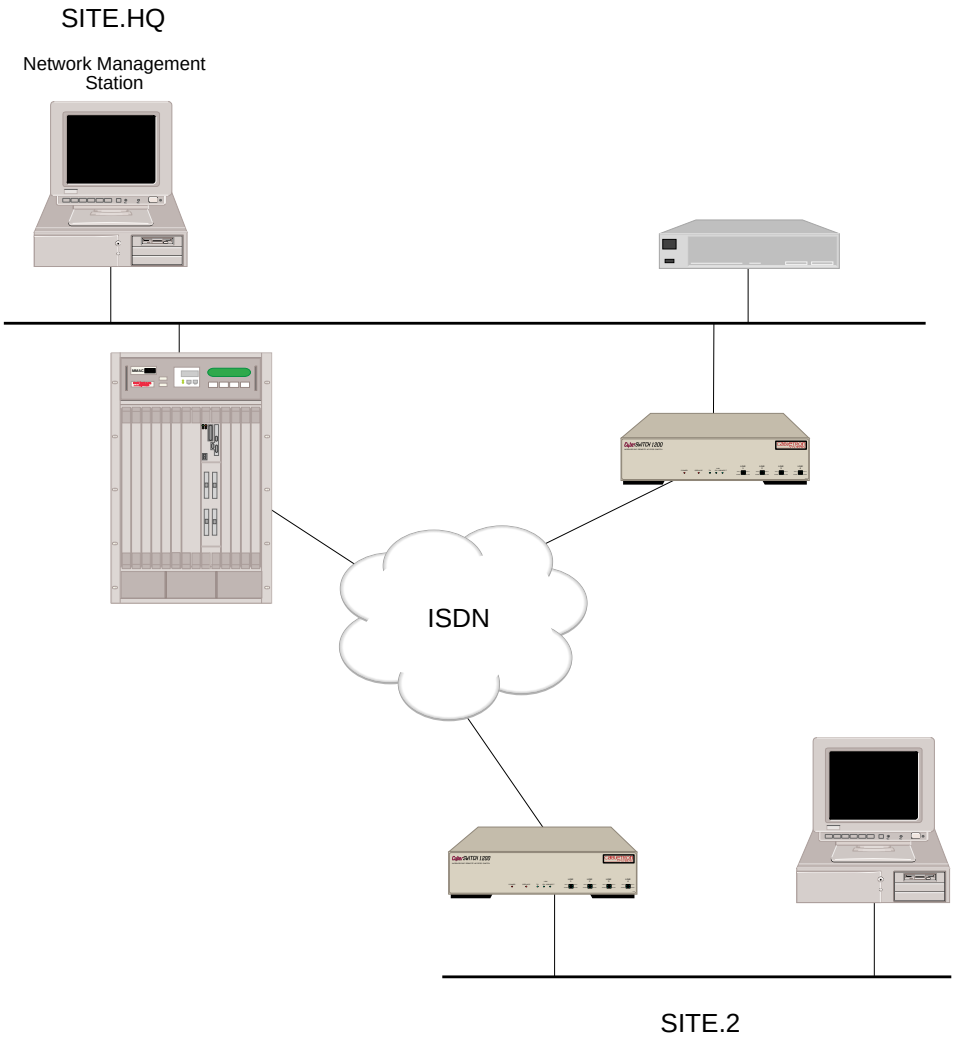
For information on first-time access (either local or remote), refer to *Accessing the SmartSwitch Remote Access Module*.

The SmartSwitch Remote Access Module has various tools to manage the system remotely. You may combine several of these tools to provide a complete, customized remote network management system. In this chapter we will describe the tools, and explain several options to manage your system.

These tools are:

- SNMP (Simple Network Management Protocol)
- Telnet
- WIN95 Dial-up Networking
- TFTP (Trivial File Transfer Protocol)
- Carbon Copy

SNMP



SNMP: The NMS gathers information (including problem reports) from any SmartSwitch Remote Access Module

SNMP (Simple Network Management Protocol) is a standard way of monitoring communication devices in IP networks. With SNMP, you purchase and then set up a Network Management Station (such as SPECTRUM® or SPECTRUM® Element Manager™) for your environment. This Network Management Station (NMS) is then used to monitor your network. From the NMS you can look at information from all the SmartSwitch Remote Access Modules and other remote devices. You can detect problems without manually check each machine to see if it is working correctly.

INSTALLATION AND CONFIGURATION

SNMP has two basic components: the *SNMP Agent*, which is executed on the SmartSwitch Remote Access Module, and the *Network Management Station (NMS)*, which you purchase separately for the

environment. This section will describe how to install and configure the SNMP Agent. Refer to the specific NMS documentation for its installation instructions.

SNMP must be configured through SFVRA-CFG. Before configuring the SNMP Agent, you must have the following information:

- the Community Name(s) used in SNMP request messages generated by the NMS;
- the IP address of the NMS; and
- the Community Name to be used in Trap messages received by the NMS.

To properly configure the SNMP Agent on the SmartSwitch Remote Access Module, perform the following steps:

- enable and configure IP
- enable SNMP
- configure community name information
- configure SNMP trap information (if desired)
- change MIB-2 system group objects (if desired)

For the NMS, follow its specific installation instructions. Note that the NMS you are using must also have the latest enterprise MIB (the `ih_mib.asn` file) compiled on its system.

If you are using Cabletron's SPECTRUM® Element Manager™ as NMS, this enterprise MIB is already built into the NMS software.

If you are using a non-Cabletron product for NMS, you must perform the following:

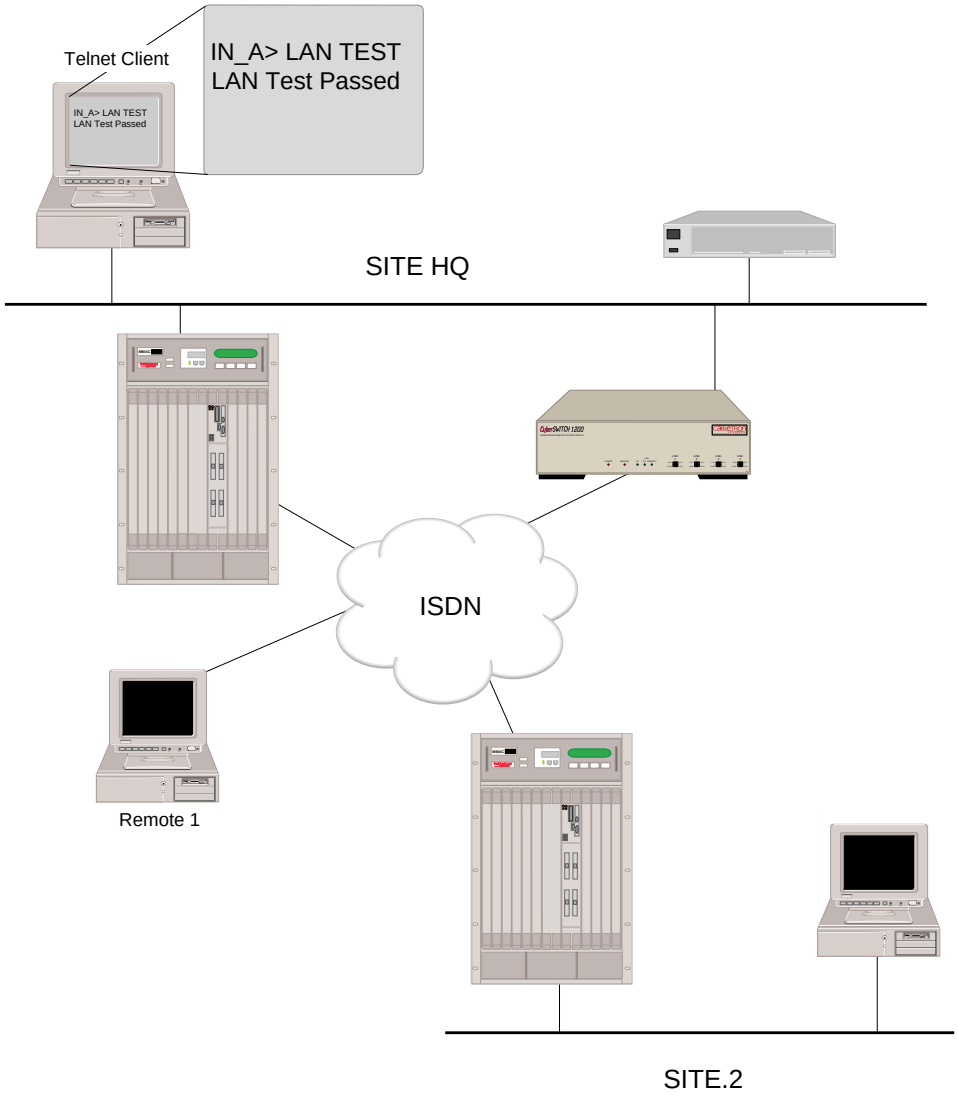
- copy the MIB file `ih_mib.asn` onto the NMS
- compile the new MIB
- set up NMS to monitor the SmartSwitch Remote Access Module

USAGE INSTRUCTIONS

Normally you will have a GUI NMS (graphical user interface) that will display a picture of the network. You will then select the desired SmartSwitch Remote Access Module and display the desired MIB information. As an example, the information displayed in the *dr* command would be located in the MIB structure under:

[private]
[enterprises]
[networkExpress]
[ih000]
[ih000StatusReports]
[ihStatusReportTable]

TELNET

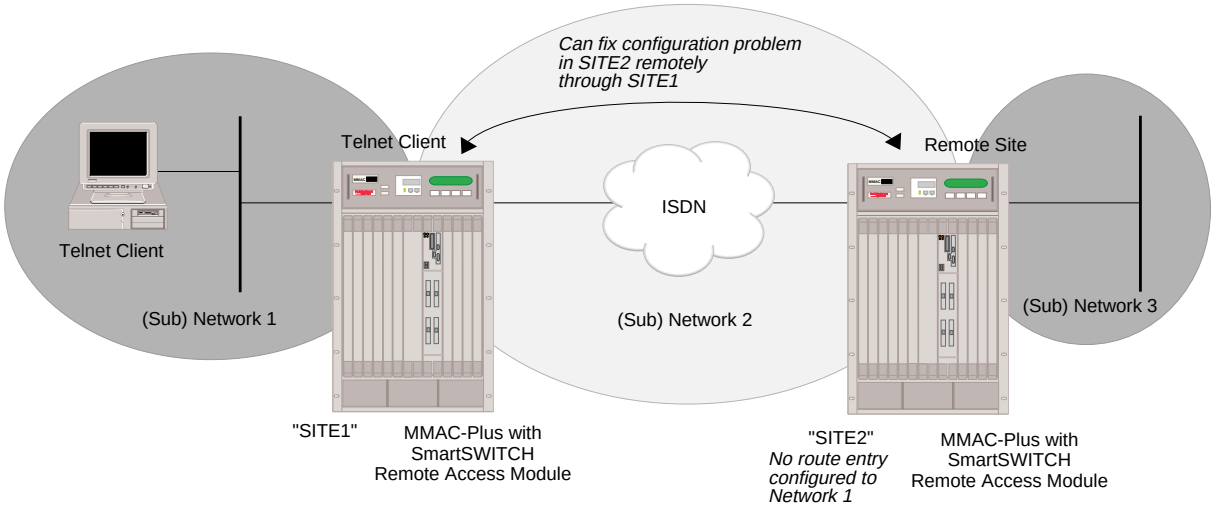


Telnet is the standard way of providing remote login service. With Telnet, any user on the LAN or WAN executing a standard Telnet client program can remotely login to the SmartSwitch Remote Access Module and get an SmartSwitch Remote Access Module console session. When you have an active console session, SmartSwitch Remote Access Module commands can be entered as if you have a locally-attached keyboard and monitor. Once you use Telnet to login to the SmartSwitch Remote Access Module, it is possible to make configuration changes to the SmartSwitch Remote Access Module using SFVRA-SFG.

In the first Telnet illustration (see previous page), the Telnet client is not an SmartSwitch Remote Access Module. It is also possible to use the SmartSwitch Remote Access Module as the Telnet client. This allows you to remotely manage an SmartSwitch Remote Access Module with an SmartSwitch Remote Access Module. The benefit from this is you can now use an SmartSwitch

Remote Access Module at your site to perform system maintenance, for example configuration changes, on a remote SmartSwitch Remote Access Module.

The picture below illustrates the advantage of the SmartSwitch Remote Access Module Telnet client feature. The example network shown illustrates that system 1 has Telnet client capabilities, and therefore can simply Telnet to System 2 and add the needed static route.



INSTALLATION AND CONFIGURATION

Telnet is available by default when IP routing is enabled. No installation or configuration steps are required.

USAGE INSTRUCTIONS

To access the SmartSwitch Remote Access Module using Telnet, you must have a Telnet client software package. A Telnet client software package is built into the SmartSwitch Remote Access Module. With the SmartSwitch Remote Access Module acting as the Telnet client, simply enter the *`telnet <ip address>`* command to Telnet into the target host. Refer to the *System Commands* chapter for a complete listing of available Telnet commands.

If you are using a PC or a workstation as a Telnet client, it must have a Telnet client software package. From the Telnet client package, issue the command that will allow you to connect to the IP address of the SmartSwitch Remote Access Module. You will then be presented with the "`Enter Login id:`" prompt. Now enter commands as if directly connected to the SmartSwitch Remote Access Module.

When finished with the session, enter the *`exit`* command at the system prompt to end the session with the SmartSwitch Remote Access Module.

Terminate the Telnet session by typing *`logout`*. This will ensure that the Telnet session has been terminated, regardless of the specific Telnet client used.

Notes: If you need to quit then restart the SmartSwitch Remote Access Module for some reason issue the *restart* command. Then reestablish your Telnet session.

If you lose your Telnet connection within 10 seconds of entering the *restart* command, the command will not be executed.

WIN95 DIAL-UP NETWORKING

Many dial-up client software packages support a terminal type of connection. One such popular package is Win95 Dial-Up Networking. The SmartSwitch Remote Access Module can handle these terminal-type connections through its digital modem feature, thus providing yet another means of remote management.

This section describes how to set up Win95 dial-up networking for a terminal-mode connection to the SmartSwitch Remote Access Module. Specifically, it details:

- the setup of a new number for dial-up networking
- the process of dialing a newly set-up number

SETTING UP A NEW NUMBER

On the remote PC running Windows 95 software:

1. Click *Start*, *Programs*, *Accessories* and then *Dial-Up Networking.* (Or, you may get to the same location by clicking *My Computer*, then double clicking on *Dial-Up Networking*).
2. Double click on *Make New Connection*:
   - Provide name of the computer you are dialing to, and
   - Select modem type
3. Click *Configure*. Three tabs will be displayed:
   - *General* tab:
     - Select com port to which your modem is hooked up.
     - Select modem's maximum speed.
   - *Connection* tab, *Connection Preferences*:
     - Set the following: *Data Bits*, *8*; *Parity*, *none*; *Stop Bits*, *1*.
     - *Port Settings* and *Advanced* may remain at default values.
   - *Connection* tab, *Call Preferences* may remain at default values.
   - *Options* tab should remain at default values for PPP connections; for remote management, select *Bring up terminal window after dialing*
4. Click *OK* to accept these values and return you to the modem name / type screen. Click *Next*.
5. Provide *Area code* and *Phone number* of the network you are trying to dial. Also identify the country of the network Click *Next*.
6. Confirm your choices. Click *Finish* to proceed, or *Cancel* to abort the new number shortcut.

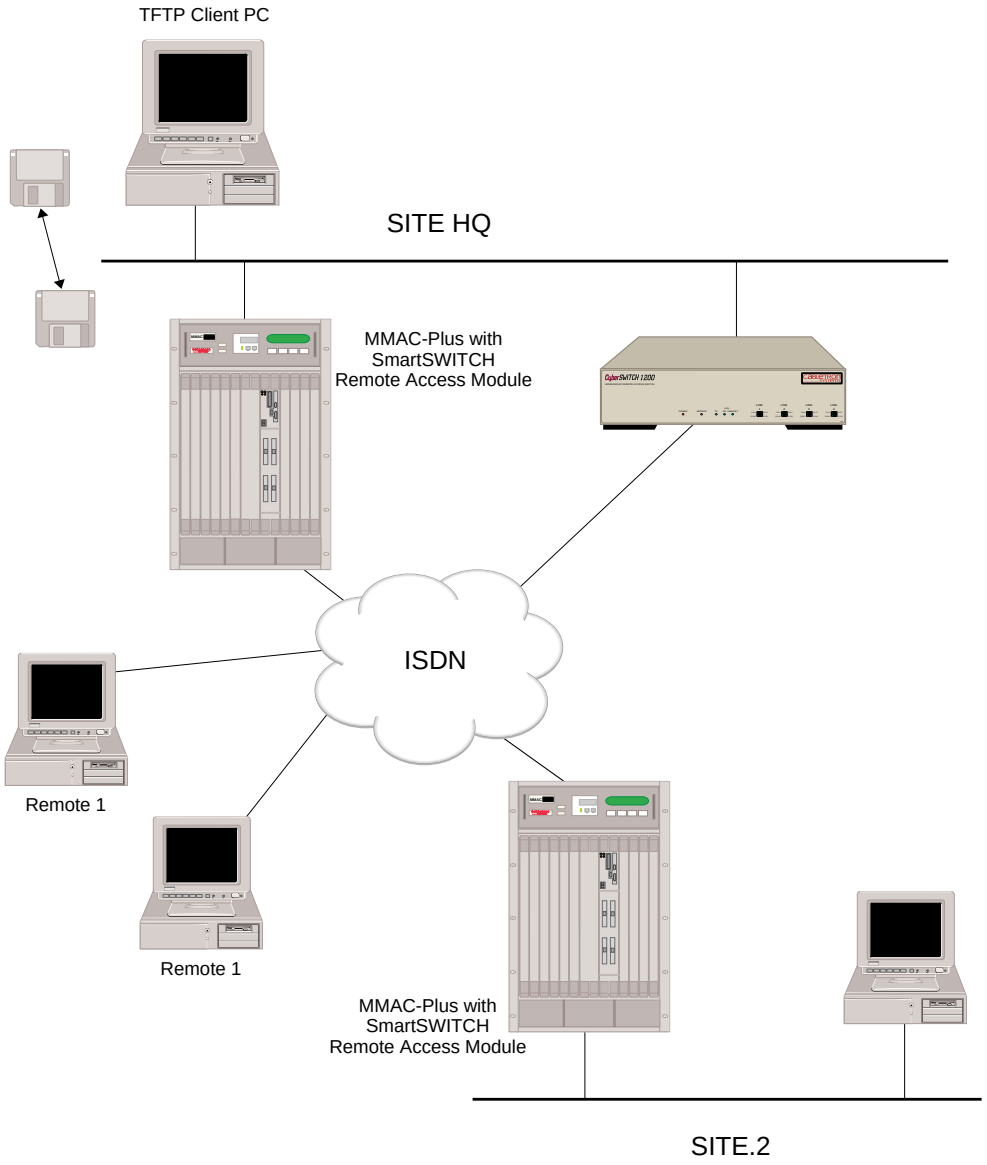
SETTING UP SERVER TYPE

1. After setting up a new number, a new dialing icon will be displayed under *Dial-Up Networking*. (It will have the name you've assigned the new connection). Select this item, click *File*, and then *Properties*.
2. Click *Server Type*. Pick options you want, and identify which protocols your network allows.
3. Click *TCP/IP Settings*. Click *Specify an IP Address* and provide the IP address of your machine. Click *OK* when finished.

DIALING OUT

1. Double click on your new dialing icon to bring up the *Connect To* screen.
2. Enter your user name and password. You may change options by clicking the box labelled *Dialing Properties*, but this isn't necessary.
3. Double click on *Connect*. This should place the call.

TFTP



TFTP (Trivial File Transfer Protocol) is the standard way of providing file transfers between devices. With TFTP any WAN or LAN user executing a standard TFTP client program can transfer files to and from the SmartSwitch Remote Access Module. You can control access to the different file types. Statistics concerning the file accesses are available. This feature can be used to retrieve report and statistics files, and to perform remote node configuration.

INSTALLATION AND CONFIGURATION

TFTP is available to the user by default. No installation or configuration steps are required.

The default file access for the GUEST user is "read" access to all files. The default file access for the ADMIN user is "read" access to the report and statistics files, and "read and write" access to all other files. The default for the TFTP server is ADMIN file access rights. The possible file types and possible accesses for each user are:

Users	*Report Files*	*Statistics Files*	*Config files*	*Other Files*
GUEST	RN	RN	RN	N
ADMIN	RN	RN	RWN	RWN

where:
"R" for *read only* file access
"W" for *write* file access
"N" for *no* access rights for the corresponding file type

Actual files included in the file type categories are as follows:

File category	*File types included in the category*
Report	RPRT_LOG.1 - 10
Statistics	STAT_LOG.1 - 10
Configuration	*.NEI (with the exception of CFGTOKEN.NEI)
Other	All other file types: .EXE, .COM, .TXT, (CFGTOKEN.NEI), etc.

Note: If you use TFTP to copy over configuration files to the SmartSwitch Remote Access Module, the new configuration will not take place until the SmartSwitch Remote Access Module is restarted. This may be accomplished with Telnet session and issuing the `restart` command. The Telnet session must then be reestablished.

USAGE INSTRUCTIONS

The SmartSwitch Remote Access Module has both the client and server TFTP components built into it. When using the SmartSwitch Remote Access Module as the local client, enter the following command(s) to transfer files:

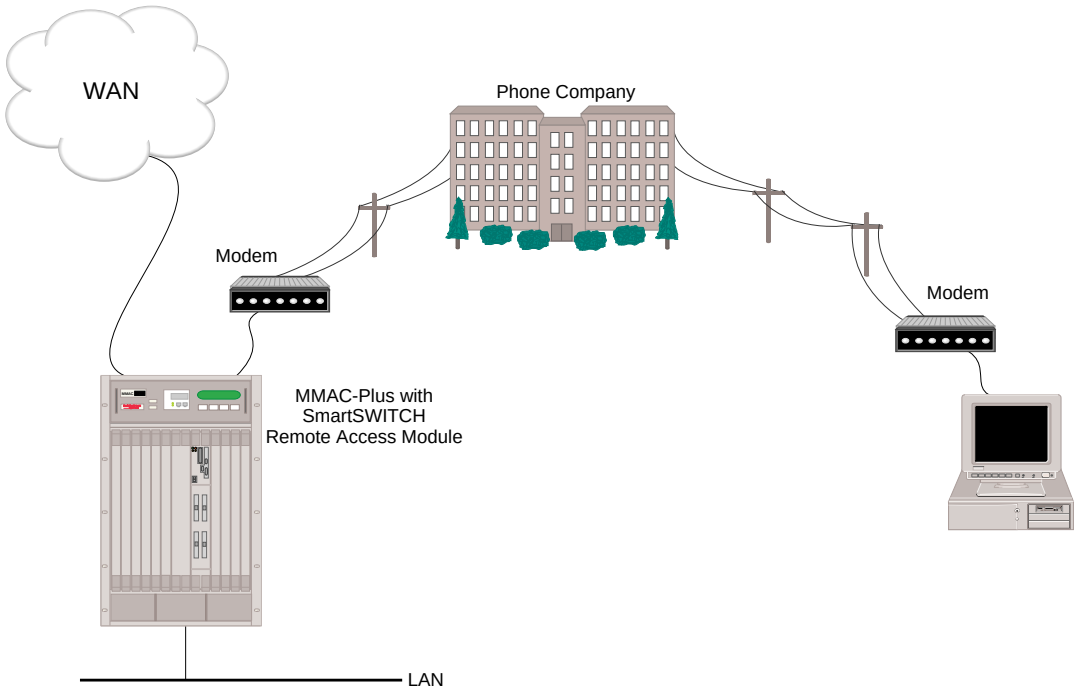
`tftp put` or `tftp get`

The `tftp put` command transfers files to the remote host; the `tftp get` command retrieves files from the remote host. For either command you will then be prompted for the IP address of the remote host, the complete path of local file name, the complete path of the remote file name, and the file mode (binary or ASCII). You will be notified of the status of the transfer.

There is a `tftp stats` command that gives the user statistics on the TFTP feature. Statistics for the server (or remote) side imply that someone from a remote device (either on the LAN or WAN) initiated the request to transferred files to (or from) the SmartSwitch Remote Access Module. Statistics for the client (or local) side imply that the user on the SmartSwitch Remote Access Module initiated the request to transfer files to a remote device. The following statistics are available for both the server and client sides:

- Number of successful file puts
- Number of successful file gets
- Number of failed file puts
- Number of failed file gets
- Total bytes put
- Total bytes get

CARBON COPY



The Carbon Copy feature gives you complete remote management. Any command that you can issue on a local console session can be issued with Carbon Copy. Files can also be transferred between the Manager PC and the SmartSwitch Remote Access Module.

The disadvantage of using Carbon Copy is that a separate telephone line must be connected to each SmartSwitch Remote Access Module being managed. Another disadvantage is that the Manager PC must be an AT compatible PC.

INSTALLATION AND CONFIGURATION

When using the Modem Remote Administration Console, the connection to the SmartSwitch Remote Access Module is done using standard modems. Modems and cables are NOT provided with the SmartSwitch Remote Access Module.

When an SmartSwitch Remote Access Module is delivered, Carbon Copy is configured for a Direct Remote Administration Console. To set your system up for a Modem Remote Administration Console, you must reconfigure Carbon Copy's baud rate and modem type parameters. Instructions for changing these parameters are listed below.

CHANGING CARBON COPY CONFIGURATION PARAMETERS

The Carbon Copy *CCINSTAL* program is available on the SmartSwitch Remote Access Module and on the Manager diskette. (The diskette is available as an option when you order your SmartSwitch

Remote Access Module). You can use this program to change Carbon Copy parameters such as password, COM port, baud rate and modem type.

To change Carbon Copy parameters on the SmartSwitch Remote Access Module, terminate the SmartSwitch Remote Access Module by typing ***quit***. Next, enter the following command at the MSDOS prompt to change the current directory to "ADMIN":

C:\>cd \admin

Enter the following command to start up the *CCINSTAL* program:

C:\admin>ccinstal

The Carbon Copy System Parameters screen will appear. Follow the directions on the screen to change parameter settings.

```
A   Comm Port Address  COM1                    Q   Quit, changes not saved
B   Baud Rate          9600                    X   eXit, changes saved
C   Modem Type         Direct Connect
D   Keyboard Handling  USA Keyboard
E   Display Type       Default
F   Menu Colors        White on Blue
G   Working Directory  Default Directory
H   Menu Level Option  Advanced

1   CC Optional Configuration Parameters
2   CCHelp Optional Configuration Parameters
3   Call Table
4   Password Table


    Type letter for selection:
```

After you make all parameter changes, select "X" to save the changes and exit the *CCINSTAL* program. Restart the SmartSwitch Remote Access Module by issuing the command: ***start_ne.*** After issuing the ***start_ne*** command, you must again login to the system.

CARBON COPY CONFIGURATION PARAMETERS FOR MODEM USAGE

If you wish to manage your SmartSwitch Remote Access Module via a modem, you will need to make changes to the Carbon Copy configuration parameters. To make these configuration changes, you must have previously installed your internal or external modem. You will also need a locally attached keyboard and monitor.

To change Carbon Copy parameters on the SmartSwitch Remote Access Module, terminate the SmartSwitch Remote Access Module by typing ***quit***. Next, enter the following command at the MSDOS prompt to change the current directory to "ADMIN":

C:\>cd \admin

Enter the following command to start up the CCINSTAL program:

C:\admin>***ccinstal***

The Carbon Copy System Parameters screen will appear. Refer to the above section titled *Changing CARBON COPY Configuration Parameters* for a sample screen. Follow the directions on the screen to change parameter settings. The parameters that you may need to change are as follows:

Modem Type
You must change the modem type from the default of "Direct Connect" to your modem's brand name. To make this change, enter a menu selection of "C" (for Modem Type). A list of modem types will be displayed. Arrow down to the type of modem you have installed. If the type of modem you have installed is not included on the list, select Hayes Smartmodem.

You will then be asked if you want to use the Modem's default baud rate. Answer either yes or no by entering Y or N.

Baud Rate
If you wish to enter a new baud rate, enter a menu selection of "B "(for Baud Rate). Continue to press B until the baud rate you desire is displayed.

When you have finished making Carbon Copy configuration parameter changes, enter a menu selection of "X" to save your changes and exit the *CCINSTAL* program. You will be asked if you wish to update the presently running Carbon Copy. Enter "Y" for yes. Carbon Copy will then be reinitialized and you will be returned to the MSDOS prompt.

USAGE INSTRUCTIONS

ESTABLISHING A REMOTE ADMINISTRATION SESSION

When using the remote administration console option, Carbon Copy establishes an administration session with the SmartSwitch Remote Access Module. This section contains a brief description of establishing an administration session using Carbon Copy.

1. If you did not install the Manager software onto the administration console PC (see *Upgrading System Software*) then insert the Manager software diskette into the diskette drive on the administration console PC.

2. Set the administration console PC to the disk drive containing the Manager software (replace "drive letter" with the appropriate administration console PC drive, for example, "A" or "C"). Type:
   ```
   <drive letter>:<return>
   ```

3. Set the administration console PC to the directory containing the Manager software. Type:
   ```
   cd \admin<return>
   ```

4. Load the Carbon Copy CCHELP program on the administration console PC. Type:
   ```
   cchelp<return>
   ```

   Within 3 to 10 seconds, Carbon Copy will be displayed on the screen. The screen is divided into three sections. In the lower right hand corner is the Carbon Copy command screen. It is function-key driven and provides the following commands:

```
[F1]          Call CC Device
[F3]          Capture Screen/Session
[F4]          Review/Replay Captured Image
[F6]          Printer/LOG/DOS Control
[F7]          Terminal Emulation
[F8]          Data Link Maintenance
[F10]         Return to Application
```

5. Choose `Call CC Device` from the Carbon Copy command screen.
   Press: <F1>

   The system will prompt you for a phone number. If you are using remote access with modems, then enter a phone number. If you are directly connected with a null-modem cable, then no phone number is required; just press the enter key.

6. Type: <phone number><return>
   (or just <return> if directly connected)

   The system will prompt you for a password. The default password set on each SmartSwitch Remote Access Module is "CC". We recommend that you change this password on each SmartSwitch Remote Access Module using the CCINSTAL program.

7. Type: cc<return>
   (or <your password><return> if the password has been changed)

   If connection with the SmartSwitch Remote Access Module is successful, then the system will remove the Carbon Copy screen. An active administration session now exists with the SmartSwitch Remote Access Module.

   If connection with the SmartSwitch Remote Access Module is not successful, then the system will return an error message in approximately 60 seconds. Check the cable connections, phone number, and password. If the connection with the SmartSwitch Remote Access Module is still unsuccessful, report the problem by using the procedures defined in *Getting Assistance*.

TERMINATING A REMOTE ADMINISTRATION SESSION

This section tells you how to terminate a remote administration session from the administration console PC. You may need this information if you want to make changes to an SmartSwitch Remote Access Module, and then use the same administration console PC to access a different SmartSwitch Remote Access Module.

1. Return to the Carbon Copy command screen.
   Press: <ALT><RIGHT SHIFT> (at the same time)

   This will return the user to the Carbon Copy main screen. In the lower right hand corner, the following commands will be displayed. This command menu is function-key driven.

```
[F1]          Terminate Link
[F3]          Capture Screen/Session
[F4]          Review/Replay Captured Image
[F5]          File Transfer Package
[F6]          Printer/LOG/DOS Control
[F8]          Data Link Maintenance
[F9]          Repaint Screen & Return
[F10]         Return to Application
```

2. Choose "`Terminate Link`" from the Carbon Copy command menu. Press:
   <F1>

3. Carbon Copy will ask if you really want to terminate the link. To answer yes, press:
   <return>

4. Choose "`Return to Application`" from the Carbon Copy command menu. Press:
   Press: <F10>

Performing a File Transfer Using CARBON COPY

After a successful Carbon Copy logon, the lower right hand corner may contain the Carbon Copy menu. If the menu is not present, display it by pressing the <ALT> and <RIGHT SHIFT> keys simultaneously.

```
[F1]          Terminate Link
[F2]          Switch Voice to Data Mode
[F3]          Capture Screen/Session
[F4]          Review/Replay Captured Image
[F5]          File Transfer Program
[F6]          Printer/LOG/DOS Control
[F7]          Terminal Emulation
[F8]          Data Link Maintenance
[F10]         Return to Application
```

To initiate the File Transfer Program, press the function key <F5>.

The file transfer facility will display a one page tutorial. The administration console PC is considered the LOCAL PC. The SmartSwitch Remote Access Module is considered the HOST. To copy files, you issue a command similar to a standard MSDOS copy command and supply the proper prefix to the file paths. For example:

COPY LC:NETWORK.NEI HC:\CONFIG\NETWORK.NEI

where:
L=Local
H=Host

This command will copy the NETWORK.NEI file from the current directory on the administration consoles PC's C: drive to the SmartSwitch Remote Access Module's C:\CONFIG directory. This downloads files from the administration console PC to the SmartSwitch Remote Access Module. To retrieve files such as system logs from the SmartSwitch Remote Access Module, simply reverse the copy procedure.

If you find you need to create subdirectories, rename files, type documents, or other similar file manipulations, you can do so without leaving Carbon Copy. The file transfer facility offers DOS command equivalents to RENAME, TYPE, MKDIR, DIR, and several other popular file manipulation commands. Simply type HELP at the prompt to get more information.

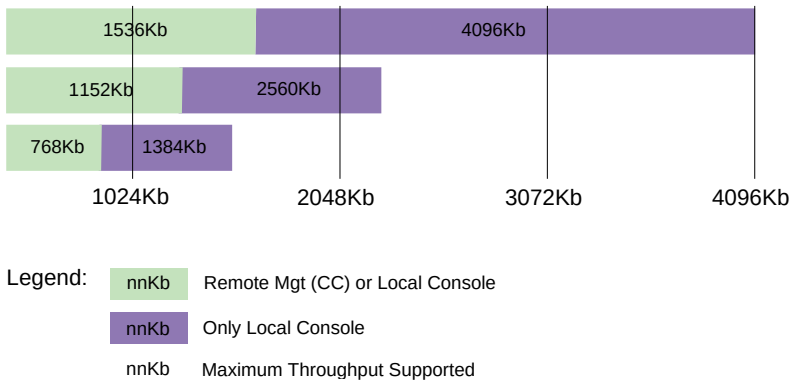
After you finish copying files and want to log-off, select Terminate Link from the command menu. Press: <F1>.

Then select Return to Application from the command menu. Press <F10>. This will return you to the DOS prompt.

RUNNING WITHOUT CARBON COPY

If you plan to use one or more dedicated links of 1Mbps or more, you may wish to increase your system's performance by running without Carbon Copy.

For each Platform, the chart below compares the maximum throughput supported with remote management (running Carbon Copy) compared to the maximum throughput supported with running only a local console (running without Carbon Copy). As shown, the higher the maximum throughput supported, the greater performance improvement there is when Carbon Copy is not running.



Note: The above graph represents the guaranteed throughput without CRC errors. The actual throughput may be higher.

REMOVING CARBON COPY

To remove Carbon Copy from your system:

1. QUIT from the SmartSwitch Remote Access Module.
2. At the DOS prompt, type "dropcc".
3. Reboot your SmartSwitch Remote Access Module.

NULL MODEM CONNECTION

To use Carbon Copy via a local NULL modem connection to make configuration changes, follow the steps listed below:

1. Insert Disk 1 from your Installation or Upgrade disk set labeled R2.3I13 or later, and reboot.
2. Carbon Copy will now be available via a NULL modem connection to the Serial Port.
3. Once the configuration changes have been made, remove the floppy and reboot your SmartSwitch Remote Access Module. Running the system with Disk 1 inserted is not recommended.

ADDING CARBON COPY

If you wish to restore remote management to your system, re-add Carbon Copy by following the steps below:

1. QUIT the SmartSwitch Remote Access Module.
2. At the DOS prompt, type "addcc".
3. Reboot your SmartSwitch Remote Access Module.

Note: Carbon Copy is a registered trademark of Microcom Systems, Incorporated.

SYSTEM COMMANDS

OVERVIEW

Two classes of system administration commands are available on the SmartSwitch Remote Access Module: guest commands and administrator commands. Guest commands provide current operational information only, and are available to all security levels. Administrator commands allows access to the complete system command set.

You need an active administration session to issue these commands. Instructions for establishing an administration session are provided in *Accessing the SmartSwitch Remote Access Module*.

The log-in to the system controls command access. Each access level (guest or administrator) is protected by a unique log-in password. This capability allows managers to assign different responsibility levels to their system administrators.

General operation commands immediately follow this discussion. These commands are divided by functions. Specific feature commands begin on page 209. These commands are arranged alphabetically. For a tabularized listing of system commands, refer to the *Command Table*.

Note: When there are a group of related commands, a help screen is available. For example, to display the help screen for all of the `br` commands, enter `br?` at the system prompt.A screen will then be displayed that includes the available br commands, the syntax for each command, and a definition for each command.

ACCESSING ADMINISTRATION SERVICES

SmartSwitch Remote Access Module software must be running in order to access Administration Services. To start the system, type `start_ne` at the DOS prompt.

The following commands are available for system login:

`admin`

Logs you into the system and provides access to all system commands. The system will ask you to enter or set the password for administrator level access. Be careful, passwords are uppercase and lowercase sensitive.

`admin<00><01><02>...<99>`

If you have configured multiple administration login names on your off-node server, you must use one of the configured names to log into the SmartSwitch Remote Access Module. The acceptable names are *admin00* through *admin99*. Proper login provides you with access to all system commands. The system will ask you to enter or set the password for administrator level access. Be careful, passwords are uppercase and lowercase sensitive. (Note: This command is not available for local access.)

`guest`

Logs you into the system and allows the user access to the commands for viewing operational information only. All other commands for changing information on the system are not

available. The System will ask you to enter or set the password for guest level access. Be careful, passwords are uppercase and lowercase sensitive.

exit
Terminates the administration session by logging-out the current administrator. You can start another session by using one of the two log-in commands outlined above.

logout
Terminates the administration session by logging-out the current administrator. You can start another session by using one of the two log-in commands outlined above.

pswd
Changes the password for the current access level (administrator or guest). Your password must be a 3 to 8 nonblank character string. Be careful, passwords are uppercase and lowercase sensitive.

SETTING THE IP ADDRESS

The following administrative command allows you to make changes to the system's default IP address without using the CFGEDIT utility. The system handles this command as if you were in CFGEDIT mode, and saves changes automatically. You must then *restart* your system in order to have these saved changes take effect. To change the system's default IP address, issue the following command:

ipconfig
Allows you to change default IP address information by prompting you for the following:
- IP address
- number of significant bits in subnet mask
- IP address of default gateway (or "0" if none)

After responding to the prompts, the system will ask you if you wish to restart the system in order to put into effect these changes.

VIEWING OPERATIONAL INFORMATION

The following commands are used to view system operational information:

?
Displays a help screen outlining all of the commands that are available.

br stats
Displays the current system packet statistics. Refer to *Bridge Statistics*, for a list of available statistics and their definitions.

cls
Clears the administration screen.

cs
Displays the list of connected devices along with the data rate for each device. The output for this command contains the connection time for each device along with a detailed breakdown

(per connection type) of channel usage and available data rates. If there is at least one device connected, the display will look as follows. Note that a "more" mechanism will be used when the number of connected devices exceeds a full screen. If there are no devices connected, the *cs* command does not produce any output.

```
[System Name]> CS

                Number of Channels       Data Rate (Kbps)      Connect Time
Device Name      Swi Ded FrR X25 Tot   Swi Ded FrR X25   Tot (hr:min:sec)
---------------   ------------------   --------------------   -----------
Tokyo              1   0   0   0   1    64    0   0   0    64    00:31:39
Ann Arbor          1   1   0   0   2    64   64   0   0   128    12:22:18
New York           4   0   0   0   4   256    0   0   0   256    04:02:22
```

dr

Displays reports of system messages. Refer to the chapters titled *System Messages* or *Trace Messages* for message definitions.

ds

Displays system statistics. For details on the available system statistics refer to the *System Statistics* chapter.

list [file name]

Displays the indicated file.

For example, to display the Release Notes, enter the following command:

```
list rel_note.txt
```

The "more" mechanism is used to view the indicated file. To view the next section of the file, simply press any key (except *<escape>*). The system will automatically return to the normal system prompt after the entire file has been displayed. If you are viewing the Release Notes, press the *<escape>* key to exit the release notes and continue with the installation.

If the file name is incorrect, the following message will be displayed:

```
Cannot find file "file name"
```

mc

Displays the Connection Monitor screen. This screen provides information on the remote sites to which the system is currently connected. The system updates the display as connections are added or removed.

To display the Connection Monitor screen, Telnet and the terminal emulator must both be set as the same terminal type. Use the *term set* command to do this.

Note: The *mc* command is also available if you are remotely connected to the SmartSwitch Remote Access Module by Telnet.

neif

This command will display the system interface table. This table provides information for each of the system's physical interfaces, including interface name, interface type, slot and port number, and the operational status of each interface (up or down). This information can help to determine system problems by identifying those physical interfaces that are not operating as expected. Refer to the following example:

```
[System Name]> NEIF

id Name              Type              Slot        Port        Status
-- ----              ----              ----        ----        ------
1   Ethernet Port 1   Ethernet          3           1           up
2   Ethernet Port 2   Ethernet          3           2           down
3   BRI.LINE.1        BRI D-Channel     1           1           up
4   BRI.LINE.1        BRI D-Channel     1           2           up
5   V.35.LINE         V.35              2           1           down
```

The definitions of the interface types and the associated status possibilities are as follows:

Ethernet
Each Ethernet port is considered an Ethernet interface. An Ethernet interface is "up" if the Ethernet port is capable of forwarding packets to/from the LAN. An Ethernet interface is "down" if the Ethernet port cannot be used to forward packets to/from the LAN.

Primary Rate (D-Channel)
Each Primary Rate line which contains at least one data link is considered a Primary Rate (D-Channel) interface. A Primary Rate (D-Channel) interface is "up" if at least one data link associated with the interface is "up." A Primary Rate interface is "down" if none of the data links associated with the interface is "up."

Primary Rate (Robbed Bit)
Each Primary Rate line that uses Robbed Bit Signaling is considered a Primary Rate (Robbed Bit) interface. A Primary Rate (Robbed Bit) interface is "up" if the serial layer 1 is "up" for the line. A Primary Rate (Robbed Bit) interface is considered to be down if the serial layer 1 is "down" for the line.

Primary Rate (Permanent)
Each Primary Rate line which is used by a dedicated access is considered a Primary Rate (Permanent) interface. A Primary Rate (Permanent) interface is "up" if the serial layer 1 is "up" for the line. The dedicated access does not have to be "up" for the interface to be considered "up". A Primary Rate (Permanent) interface is considered to be down if the serial layer 1 is "down" for the line.

sp

This command pertains to semipermanent connections. This command will list each semipermanent device, as well as the connection status, initial data rate and current data rate for each semipermanent device. The connection status will be one of the following:

CONNECTED
The system is connected to the device at the initial data rate or greater.

OVERRIDDEN
The *disc device* command was issued on this device. The system will not attempt to call again until a *call device* command is issued, or the system is rebooted.

NOT CALLABLE
This device cannot be called. Check phone number, device type or existence of the device name in the database.

REJECTED
The remote device answered the system call, but rejected negotiations. The system stops calling attempts until a `call device` command is issued, or the system is rebooted.

TRYING
The system is attempting to call the device. Some connections may be up, but not at the initial data rate.

`status`
Displays initialization, current status, and connection information, as well as any errors that have been detected.

`time`
Displays the current system time. This can be useful when viewing system messages or statistics.

`ver`
Displays the version number of the software that is currently running on the system (II, III, etc.). In addition, it displays all other custom information for this copy of the system software, such as the platform, the installed resources, and the hardware resource revision information. Note that T1_E1_PRI-1 indicates the PRI-23/30 adapter.

The *ver* command also displays a connections table. It displays the connection lines for features that are loaded only. Consider the following example of a connections table:

Capacities	Potential	Actual
Physical Connections	8	8
X.25 Connections	32	32
Frame Relay Connections	48	33
Combined Maximum Connections	88	33

Description:
- The first column is the *connection type*.
- The second column is the *potential number of connections*.
- The third column is the *actual number of connections possible*. The actual number may differ from the potential number due to memory constraints.
- The *combined maximum* line shows the maximum number of connections possible for all types combined. If the potential and actual column do not match on this line, then there are not enough connections for all the connection types to use their respective maximum number of connections at the same time.

For our example, the most connections possible without memory limitations is 88. This is the sum of all the connection types. Since there is not enough memory for 88, the actual number of

connections available is less than that amount (33). This means that any of the following combinations of connections would be allowed:

Physical Connections	X.25	Frame Relay
8	25	0
0	32	1
0	0	33
2	2	29

If there was enough memory for all connections, the connection table would reflect both potential and actual connections as the same number.

wan stats
Displays the current system WAN connection statistics. Refer to *WAN Statistics*, for a list of available statistics and their definitions.

From the "Connection Monitor" screen you can press:

<Arrow Keys>
To select a site that is currently connected.

<Enter>
To view throughput monitoring for the selected site. Refer to the section titled *Viewing Throughput Information,* for details.

<Esc>
To exit the Connection Monitor screen.

VIEWING THROUGHPUT INFORMATION

The Throughput Monitor screen displays the system throughput monitoring feature in action. To enter this screen:

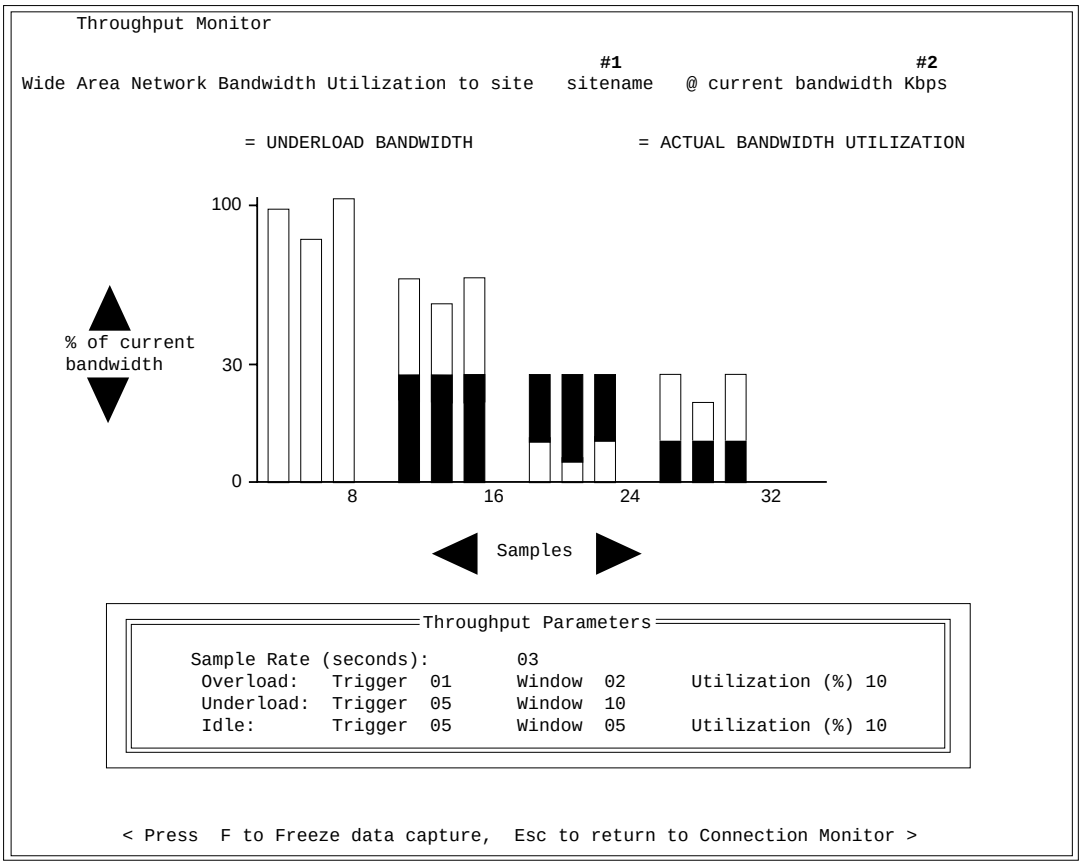
1. Issue the *mc* command to display the connection monitor screen.

2. Use the <arrow keys> to move the cursor down to the specific site for which you would like to view throughput information.

3. Press <enter> to display the throughput monitor screen for that site.

Throughput monitoring information can be very useful for fine-tuning your bandwidth configuration parameters. Note that this feature is not available through a Telnet session. Refer to the *Configuring Call Control* chapter of the Central Site CSX user documentation for a complete description of throughput parameters.

The actual bandwidth utilization, along with the current underload setting, is displayed for each throughput sample. After 32 samples are displayed, the newest sample is displayed at position 32 and all other samples are shifted left one position.



Note: If data compression is being used, an extra line will be displayed on the Connection Monitor screen that will provide the compression and decompression ratios, and the estimated throughput. The estimated throughput is calculated as follows:

est. thruput (in Kbits/second) = [(uncmp bits + undmp bits)/sample period)]/1000

Where uncmp bits = the number of uncompressed bits
undmp bits = the number of undecompressed bits
sample period = configured length of the sample period

THROUGHPUT MONITOR CONTENTS

#1. Indicates the site name for the connected site that was selected on the Connection Monitor screen.

#2. Indicates the current bandwidth in place to the connected site. This number will be updated as calls are added or released.

#3. Example of three samples where actual bandwidth utilization was around 95% and underload was not being monitored (probably because only one connection was in place). In this example, overload is occurring on all three samples.

#4. Example of three samples where actual bandwidth utilization was around 70% and underload was being monitored at around 25% utilization of current bandwidth. In this example, overload is occurring on all three samples.

#5. Example of three samples where actual bandwidth utilization was around 10% and underload was being monitored at around 25% utilization of current bandwidth. In this example, underload is occurring on all three samples.

#6. Example of three samples where actual bandwidth utilization was around 25% and underload was being monitored at around 10% utilization of current bandwidth. In this example, neither overload nor underload is occurring.

From the Throughput Monitor screen, press:

f To freeze the current throughput monitor display.

r To resume the display of throughput monitor samples.

<esc> To exit the Throughput Monitor and return to the Connection Monitor screen.

SAVING OPERATIONAL INFORMATION

The following commands are used to save system operational information to disk:

wr
Writes the current system messages to disk file.

ws
Writes the current system statistics to disk file.

Note: For details on these disk files, refer to the chapter titled *Software Overview*.

CLEARING OPERATIONAL INFORMATION

The following commands are used to clear current system operational information:

er
Erases the current system messages held in memory.

es
Erases the current system statistics held in memory.

TERMINATING AND RESTARTING THE SMARTSWITCH REMOTE ACCESS MODULE

The following commands are used to terminate and restart the system program:

quit

Terminates the system program. You may need to "*quit*" in order to perform a system function such as a system upgrade, configuration change or a configuration backup.

start_ne

Restarts the system program and is available only after you issue the *quit* command. After issuing the *start_ne* command, you must again login to the system.

restart

Generally used from a remote site (when using Telnet or TFTP), although it is functional from a local console as well. The *restart* command reboots the system and automatically starts up the system software.

If you prefer, you can make configuration changes and store them remotely. Later, you can transfer the changes (the .nei files) to the system using TFTP. In order for these changes to take effect, you would need to issue the *restart* command from the Telnet session of your remote terminal.

Note: If you lose your Telnet connection within 10 seconds of entering the *restart* command, the command will not be executed.

SETTING THE DATE AND TIME

The following commands are used to set the date and the time on the system:

date <month, day, year>

Changes the date on the system as specified. The <month> can be specified as a numeral from 1 to 12, spelled out in full (January), or abbreviated to 3 letters (JAN). The <day> can be any legal date within the month specified. (For example, 1 through 31 would be legal dates for January.) The year may be specified in its entirety (1995) or by its last two digits (95). Commas, dashes, and white space are all acceptable separators.

time hours:minutes <:seconds> <AM/PM>

Changes the time on the system as specified. The hours can be from 0 - 23 in military time, or from 1 - 12 in civilian time, with an optional AM / PM indicator. The "seconds" parameter is also optional. If "P" is included (indicating "PM"), 12 is added to the hour. White space is unimportant.

Note that if the time command is issued without any parameters, the system will report the current time. Parameters following the time command are interpreted as an attempt to make a change.

TERMINATING ADMINISTRATION SESSIONS

The following commands are used to display and to terminate active administration sessions.

`session`

This command will display the current active administration sessions. The example screen below illustrates the format in which this information is displayed:

```
Login-Id Sess-Id   Date/Time Idle(sec) Command   Type (from)
-------- -------   --------- ---------- -------   -------------------
ADMIN       0    Aug 15 13:50     51     MANAGE    Console
ADMIN     257    Aug 15 13:55      0     SESSION   Telnet (199.120.211.120)
```

The fields in this display are defined as follows:

Login-Id
The access level associated with the session. Possible access levels include:
admin: administrator access
guest: guest access
nobody: someone has initiated a Telnet session with the SmartSwitch Remote Access Module but did not login.

Note: If you have configured multiple admin login names on your off-node server, the *login-id* field will not distinguish between the various names. Use the *sess-id* field to help identify the different admin users.

Sess-Id
The session Id number associated with the session.

Date/Time
The date and time the session was initiated

Idle (sec)
The number of seconds the connection has been idle.

Command
How the administration session was initiated. Initiation methods include:
manage - the user is in the Manage Mode
session - the user is using a Telnet session

Type (from)
The type of session. Possible session types include:
console - a session through the local console
telnet - a Telnet session

Note: If you have configured multiple admin login names on your off-node server, the *login-id* field will not distinguish between the various names. Use the *sess-id* field to help identify the different admin users.

`session kill <session id>`

Terminates the session specified by the session Id. Useful for terminating sessions that have been idle for an extended period of time.

APPLETALK ROUTING COMMANDS

The following commands are used to display AppleTalk information and statistics.

atalk arp

This command will display the AARP (AppleTalk Address Resolution Protocol) cache. AARP is used to map between a device's AppleTalk address and their physical address. A sample output screen is shown below:

```
Entry 1: Address 21.1 @ 08:00:07:8f:90:04, valid
```

where:

Address 21.1 is Entry 1's AppleTalk address.
08:00:07:8f:90:04 is Entry 1's physical address (MAC address).
valid is the state of Entry 1's address. The state value can be either valid or pending. If the state is valid, an address will have been logged (as shown). If the state is pending, the address would not yet be logged, and would appear as 00:00:00:00:00:00.

atalk ping <dnet>.<dnode> [timeout/dnnn]

This command will allow you to "ping" a specified device. If the ping is successful, you have connectivity to the device. If it is unsuccessful, you do not have connectivity to the device.

The parameters for this command are:

dnet
Required parameter. The destination network number.

dnode
Required parameter. The destination node Id.

timeout
Optional parameter. The number of seconds to wait for a reply message. The valid range is from 1 to 60 seconds. The default value is 10 seconds.

nnnn
Optional parameter. The data size to be included in the ping packet. The valid range for the data size is 5 to 586 octets. The default value is 100 octets.

An example atalk ping command could read as follows:

atalk ping 1.3 30 /d200

which would send a ping to node number 3 or network number 1, with a timeout value of 30 seconds, and the data size would be 200 octets.

atalk port

This command will display AppleTalk port information. A sample output screen is shown below:

```
Port 1
     type: LAN          state: UP
     address: 20.20     network range 20-21
     flags: extended   phase-2   soft-seed
     default zone: zone1
     lan port: 1    physical address: 00409A001AB3

Port 2
     type: WAN          state: UP
     address: 30.30     network range 30-31
     flags: extended   phase-2   soft-seed
     default zone: zone1

Port 3
     type: WAN UNNUMBERED state: UP
     address: 20.20 (borrowed)
     remote device: MAC4
```

The fields in this display are defined as follows:

type

The port type. Possible types are LAN, WAN, WAN UnNumbered.

Note that the WAN UnNumbered port information is *not* taken from the previously configured AppleTalk Routing port information, but is derived from the AppleTalk Routing static route configuration information.

state

The state of the port as it is in the process of coming up. Possible states include:

listen - The port is listening to see if any other routers are out on the network.

probing - The port is probing the network to see if its suggested AppleTalk address is unique, or if it is already in use.

get_info - The port is verifying network information and obtaining the default zone.

get_zones - The port s obtaining a complete zone list for the network.

get_routes - The port is requesting routes from another router on the network (if another router is present).

up - The port is ready for use.

down - The port is not ready for use.

unnum_wait_addr - This state will exist with the following scenario:
When an UnNumbered WAN port sends a locally generated packet that requires a reply, a return address is needed. But, because the port is UnNumbered, it has no address assigned to it that it can use as a return address. To remedy this, the UnNumbered WAN port will "borrow" an AppleTalk address from a local numbered port, knowing that when the reply comes, it will first come to the UnNumbered WAN port. If the UnNumbered WAN port attempts to "borrow" an address, but there are no numbered ports up, the *unnum_wait_addr* state exists; the WAN UnNumbered port is waiting for an address.

address

The port's AppleTalk address.

network range
For a LAN port, this specifies the AppleTalk network range of the LAN segment to which the port is connected. For a WAN port, this specifies the AppleTalk network range of the logical segment to which the port is connected. For NonExtended networks, the range will appear as one number (for example, 121-121). For UnNumbered ports, the range will appear as either 0-0 (nonextended networks) or 0.0-0.0 (Extended networks). Note that if the network is nonextended (phase 1), this field will be *network* (and will display a singular value) as opposed to *network range* (which displays a range).

flags
This will reflect any flags that have been activated for the indicated port. Possible flags are:
extended - This flag is triggered if a network range has been configured for the port.
phase-1 - This flag is triggered if the NonExtended network type is configured for the port.
phase-2 - This flag is triggered if the *phase-1* flag has *not* been triggered.
probe-invalid - This flag is triggered if the port sends out a probe to see if its suggested AppleTalk address is unique on the network, and a response comes back indicating that the address is already in use, and cannot be used by this port.
soft-seed - This flag is triggered if the port is *not* configured in the discovery mode (it is configured with a suggested network range). Its classification as a *soft*-seed router indicates that it does have a suggested network range, but that range can be overridden if necessary.

default zone
The port's configured default zone.

LAN port
For LAN ports only. Indicates the Ethernet resource's port number associated with this AppleTalk LAN port.

physical address
For LAN ports only. The device's MAC address.

remote device
For WAN UnNumbered ports only. The remote device configured to use this port.

`atalk port stats [clear]`

This command will display or clear current AppleTalk port statistics. Refer to *AppleTalk Port Statistics*, for a list of available atalk port statistics and their definitions.

`atalk route`

This command will display AppleTalk static route information. A sample output screen is shown below:

```
network range     distance       state      next hop    zones valid
-------------     --------       ------     --------    -----------
 225 - 226          0            good         0.0          TRUE
```

The fields in this display are defined as follows:

network range
The remote AppleTalk network range reachable through this static route. Note that if there is only a single network number instead of a range, that number will appear twice under the network range field.

distance
The number of AppleTalk routers that are traversed in order to reach the destination AppleTalk network.

state
The state of the route. Possible values are:
good - This indicates that this is a valid route.
bad - This indicates that the indicated router has not been heard from in a while; it has timed out. Therefore, it is no longer a valid route.

next hop
The AppleTalk address of the next hop device that provides access to the destination AppleTalk network. If the distance = 0, and the next hop = 0.0, this indicates that there is no router between the port and the destination. If the distance ≠ 0, and the next hop = 0.0, this indicates that the static route is over an UnNumbered port.

zones valid
For every route there is a set of associated zones. When a device has learned the complete list of zones for that route, the zones valid field will display TRUE.

`atalk stats`

AppleTalk statistics are comprised of six subgroups of statistics. The `atalk stats` command displays all six groups of the current system AppleTalk statistics. Refer to *AppleTalk Routing Statistics*, for a list of available AppleTalk statistics and their definitions.

Enter one of the following commands to display a subgroup of the AppleTalk statistics:

`atalk stats ddp`
Displays the AppleTalk Data Delivery Protocol (DDP) statistics.

`atalk stats echo`
Displays the AppleTalk Echo Protocol (AEP) statistics.

`atalk stats rtmp`
Displays the AppleTalk Routing Table Maintenance Protocol (RTMP) statistics.

`atalk stats zip`
Displays the AppleTalk Zone Information Protocol (ZIP) statistics.

`atalk stats nbp`
Displays the AppleTalk Name Binding Protocol (NBP) statistics.

`atalk stats atp`
Displays the AppleTalk Transaction Protocol (ATP) statistics.

atalk zone

This command will display AppleTalk zone information. A sample output screen is shown below:

```
zone                            network range
-----------------               -------------
zone1                              225 - 226
zone2                              236 - 237
```

The fields in this display are defined as follows:

zone
The AppleTalk zone name for the network that the AppleTalk port is connected to.

network range
Specifies the network range associated with the indicated zone.

BRIDGE COMMANDS

The following commands are used to display bridging information and statistics.

pkt mac

Enables the MAC address monitor display. The MAC Address Monitor screen displays information contained in the LAN frames that are sent over the ISDN connections. The packets represented by the displayed MAC address pairs will not be captured unless the br pkt capture feature is on (enabled).

When the MAC Address monitor is enabled, the SmartSwitch Remote Access Module inspects each LAN frame sent or received over the ISDN connections. It displays the Destination MAC Address, Source MAC Address, and Ethernet type field for each LAN frame.

```
                                MAC Address Monitor

    DEST           SOURCE        TYPE   COUNT       DEST           SOURCE        TYPE   COUNT

90409A000000    00409A001023-L    3C09   00010    00409A001023    00409A001324-R    3C09   00140
00409A001324    00409A001023-L    3C02   00141    90409A000000    00409A001000-L    3C09   00010
90409A000000    00409A002345-L    8137   00015    00409A002345    00409A003217-R    8137   00045
00409A003217    00409A002345-L    8137   00045

                              Number of Packets Received 00406
```

In the above example, the DEST field is the destination MAC address field of the LAN frame. The SOURCE field is the source MAC address of the LAN frame. Next to the source MAC address field is the location of that source address. An “L” next to the source address indicates that this address is “Local” to the SmartSwitch Remote Access Module. That is, it is attached to the Ethernet segment locally connected to the SmartSwitch Remote Access Module. An “R” next to the source address indicates that this address is “Remote” to the SmartSwitch Remote Access Module. That is, it is attached to an Ethernet segment that is connected to a remote ISDN device.

The TYPE field is Ethernet type field of the LAN frame. This hexadecimal field represents the protocol identifier for an Ethernet formatted frame. For an 802.3 formatted frame, it is the length of the data unit.

The COUNT field is the number of frames transferred for that destination address, source address, and Ethernet type combination. The total number of frames is displayed at the bottom of the screen.

To exit the MAC Address Monitor screen and disable the feature, press <Esc> on the Administration console keyboard.

br stats
Displays the current system packet statistics. Refer to *Bridge Statistics*, for a list of available bridge statistics and their definitions.

br stats clear
Clears the current system packet statistics.

CALL CONTROL COMMANDS

The following commands are used to initiate and disconnect calls to devices.

call device <device name>
Initiates a call to the specified device. The entire device name does not need to be entered; only enough letters of the name to distinguish it from any other configured device name. For example, you could enter *call device sm* if there are no other devices whose names begin with *sm*. The call device command can be used to test the Dial Out capability to a specific device. This command is available only when the Authentication mode is "On-node Device Table." Note that the device name is case sensitive.

To use this command for troubleshooting, you must use the System Call Trace feature to capture any connect and disconnect messages that are generated by issuing the *call device* command. To do this:

1. Erase the current report log by entering *er* at the system prompt.
2. Enable the Call Trace feature by entering *trace on* at the system prompt.
3. Issue the *call device <device name>* command.
4. Display the system log messages by entering the *dr* command at the system prompt.
5. Check the log report for connect messages relating to the remote device you are testing.

In response to the *call device <device name>* command, one of the following responses will be displayed:

`Calling device <device name>`
Indicates that a call request process has been initiated.

`<device name> could not be found in the Device Table`
Indicates that the device name could not be found in the table of configured device names.

`<device name> is already connected`
Indicates that a connection to a device can not be initiated if there is already a connection to that device. The call device command cannot be used to increase bandwidth for an existing connection.

`Call attempt failed`
Indicates that the request could not be executed.

`More than one match for <device name> found in the Device Table`
Displayed if you enter just part of a device name and that part could specify more than one device name. You will be prompted to enter the device name again, in a more specific manner. For example, if *`call device Sch`* is entered, and there is a device configured with the name Schultz, and a device configured with the name Schmidt, this message would be displayed. You would then need to enter at least *`call device Schu`* to successfully initiate a call to the device Schultz.

`<device name> is not callable`
Each PPP device in the device database can have one or two phone numbers at which they can be called. This message is displayed if the device has no phone number specified.

`Re-enter the name, or <RET> to cancel`
The device name must be re-entered.

`Unable to prompt for device name at this time`
Indicates that the *`call`* command would prompt you for a device name, but the necessary resources are not available. The recommended actions are as follows:

1. If possible, enter the device name on the command line.

2. If the device name cannot be entered from the command line (for example, the device name contains command line delimiters of a space, a comma, a colon, or a tab), the user can wait for a few minutes and see if any resources become available.

3. If actions 1 and 2 are ineffective, this may indicate an internal problem in the System, please inform your service representative of the occurrence.

`call peer <phone number> [data rate] [device] [bearer]`

Initiates a call to a peer at the given number. Entering the data rate, device, and bearer is optional. We describe each of the optional fields below.

`data rate`
The default data rate value for HDLC calls is *56Kbps*. The default data rate for digital modem calls is *Auto*.

`device`
The valid values are:
- `HDLC`: used for normal HDLC-ISDN calls
- `DM`: used for Digital Modem calls.

`bearer`
This field applies only to Digital Modem calls. The valid values are:
- `SPEECH` (the default if no bearer type is specified)
- 3.1KHZ

The *`call peer`* command allows you to make a connection with another device. For example, to call a site with the configured phone number of 13135552222 and a data rate of 64Kbps, you would enter *`call peer 13135552222 64.`*

To use this command for troubleshooting, you must enable the Call Trace feature to capture any connect and disconnect messages that are generated by issuing the *`call peer`* command. To do this:

1. Erase the current report log by entering *`er`* at the system prompt.

2. Enable the Call Trace feature by entering *`trace on`* at the system prompt.

3. Issue the *`call peer <phone number> [data rate]`* command.

4. Display the system log messages by entering the *`dr`* command at the system prompt.

5. Check the log report for connect messages relating to the remote device you are testing.

In response to the *`call peer`* command, you will see the following message echoed back for informational purposes:

`Calling <phone number> at <data rate>, device PPP`

The phone number will show what is sent to the switch. Any imbedded dashes will have been removed. The data rate that is used is displayed. If an invalid data rate is entered, the default of 56 Kbps will use used. Because dial out is only provided for PPP devices, the device type is always PPP.

One of the following messages will then be displayed:

`Call initiated`
This response indicates that a *`call peer`* request was performed. This does not always imply that a request reached the telephone switch.

`Call attempt failed`
This response indicates that the request could not be executed.

Note: The *`call peer <phone number>`* command will not work under the following conditions:

If PAP or CHAP is enabled and Outbound Authentication is disable, or, if the only security enabled is CLID. In either case, the SmartSwitch Remote Access Module will not be able to authenticate the remote peer. A message will appear in the log to indicate this. Use the *`call device <device name>`* command instead.

`disc device <device name>`
Disconnects all calls to the specified device. Note that the device name is case sensitive.

In response to the *disc device* command, one of the following responses will be displayed:

`Disconnecting <device name>`
Indicates that the disconnect process has been initiated for the indicated device.

`No active connection to <device name>`
Indicates that the device that you are attempting to disconnect has no active connection. The *mc* or the *cs* command can be used to view the active connections.

`<device name> could not be found in the Device Table`
Indicates that the device name could not be found in the table of configured device names.

More than one match for <device name> found in the Device Table
Displayed if you enter just part of a device name and that part could specify more than one device name. You will be prompted to enter the device name again, in a more specific manner. For example, if *call device Sch* is entered, and there is a device configured with the name Schultz, and a device configured with the name Schmidt, this message would be displayed. You would then need to enter at least *call device Schu* to successfully initiate a call to the device Schultz.

`Re-enter the name, or <RET> to cancel`
The device name must be re-entered.

`Unable to prompt for device name at this time`
Indicates that the *call* command would prompt you for a device name, but the necessary resources are not available. The recommended actions are as follows:

1. If possible, enter the device name on the command line.

2. If the device name cannot be entered from the command line (for example, the device name contains command line delimiters of a space, a comma, a colon, or a tab), the device can wait for a few minutes and see if any resources become available.

3. If actions 1 and 2 are ineffective, this may indicate an internal problem in the System, please inform your service representative of the occurrence.

CALL RESTRICTION COMMANDS

When the Call Restriction feature is enabled on the SmartSwitch Remote Access Module, the following command is available through the administration console:

cr stats
Displays the current Call Restriction statistics. Refer to *Call Restriction Statistics*, for a list of available statistics and their definitions.

COMPRESSION INFORMATION COMMANDS

Compression statistics are only available for connections that are using a compression protocol. The following commands are used to display current compression information:

cmp stats
Displays the compression statistics for all active connections. Refer to *Compression Statistics*, for a list of available compression statistics and their definitions.

cmp stats <device name>
Displays the compression statistics for the indicated device. Refer to *Compression Statistics*, for a list of available statistics and their definitions. Note that the device name is case sensitive.

cmp clear <device name>
Clears the compression statistics for the indicated device. If the device name is omitted, no compression statistics will be cleared. Note that the device name is case sensitive.

cmp clearall
Clears the compression statistics for all devices.

DIGITAL MODEM COMMANDS

These commands allow you to display active connections, display or erase digital modem statistics, add or delete individual modems and upgrade modem firmware when necessary.

modem add <slot #> <modem #>
Adds a previously-deleted modem back to the available list for devices (i.e., after testing).

modem delete <slot #> <modem #>
Deletes a modem from the available list for devices. This command is useful in the event you have a faulty modem and wish to temporarily disable it for troubleshooting purposes. Use this command in conjunction with the *modem add* and *modem status* commands.

modem reset <slot #> <modem #>
Resets the specified DM-24 or DM-30 modems on a particular slot. Does not affect other modems on the board. A modem currently in use cannot be reset. DM-8 modems cannot be reset.

modem restart <slot #>
Restarts the digital modem board (i.e., if an unrecoverable problem occurs). This command does not affect any other boards within the system.

modem stats <slot #><modem #>
Displays the digital modem statistics associated with the specified modem. For a listing of available statistics and their definitions, refer to *Digital Modem Statistics*.

modem stats clear <slot #><modem #>
Clears the digital modem statistics associated with the specified modem.

modem status <slot #>
Displays the slots that have valid digital modem (DM) boards. If the command is executed using a specific valid DM board slot, displays the modems available for usage from specified slot.

modem upgrade <slot #> <all>
Installs new modem firmware by reprogramming the specified modem's flash memory.

Periodically, you may want (or need) to add new firmware to DM-24, DM-24+, or DM-30+ modems. To do so, you would need to load the new modem file onto the SmartSwitch Remote Access Module `C:\system` directory. Then to reprogram the modems, issue the *modem upgrade* command, which upgrades all the modems on the card:

modem upgrade <slot #> <all>

Slot number refers to the slot in which the digital modem card resides, and all refers to all modems on the card. Example: *modem upgrade 2 all* upgrades all modems on the DM card in slot 2.

We recommend you monitor the upgrade process by using the *dr* console command. The upgrade process should take approximately one minute. Only after the upgrade process completes for all modems, reset the system.

Note: DO NOT DISRUPT POWER *during* the execution of the modem upgrade process! If power is disrupted, it could result in damage to the modem.

modem devices
Displays active digital modem connections by device name. Lists slot number, modem number, and in the case of the DM-24 or DM-30, lists connect parameters.

IP ROUTING COMMANDS

In order to use the following commands, you must properly configure and initialize IP routing operating mode. In addition, you must enable RIP to use the *ip rip* commands.

The following commands are used to display IP routing information:

ip addrpool
Displays the current IP address pool. There are three fields displayed: *address*, *origin*, and *in use:*
- *address*: lists the IP address in the pool
- *origin*: specifies how the IP address has come to be placed into the IP address pool. If the origin is *DHCP*, the IP address was obtained from a *DHCP* server. If the origin is *STATIC*, the IP address was manually configured via CFGEDIT.
- *in use*: specifies whether or not the IP address has been leased to a remote IP host device.

ip arp
Displays the current ARP cache table. The IP address, its corresponding MAC address, the type of ARP table (dynamic or static), and the corresponding interface name are displayed.

ip ping <host IP address> [timeout /dnnnn]
Sends an ICMP Echo message to a specified host. The parameters for this command are:

host IP address
IP address using dotted decimal notation for the target host.

timeout
Optional parameter that indicates the number of seconds to wait for an ICMP Echo Reply Message. The valid range for the time out value is 1 to 60. The default value is 10.

/dnnnn
Optional parameter that indicates the data size in bytes for the ICMP Echo message. The valid range for the data size value is 0 to 2020. The default value is 0.

Possible Results and their meanings:

`ddd.ddd.ddd.ddd is alive`
The valid ICMP Echo Reply was received from host ddd.ddd.ddd.ddd.

`No response from ddd.ddd.ddd.ddd`
No response was received from the host within the timeout value number of seconds.

ip rip interface
Displays information pertaining to the interface data that is maintained by the IP RIP protocol. The example screen below illustrates the interface information that will be displayed when this command is entered.

```
[System Name]> ip rip interface

Status:                    Active
I/F Type:                  LAN
IP Address:                192.168.1.1
Subnet Mask:               255.255.255.0
Broadcast Address:         192.168.1.255
Transmission:              Version 1
Reception:                 Version 1 or Version 2
Query Response:            Version 1
Version 2 Authentication:  Password

Status:                    Inactive
I/F Type:                  WAN - UNNUMBERED
IP Address:                0.0.0.0 (left.CSX)
Subnet Mask:               N/A
Broadcast Address:         255.255.255.255
Host Route Propagation:    N/A

Status:                    Inactive
I/F Type:                  WAN - NUMBERED
IP Address:                192.168.3.5
Subnet Mask:               255.255.255.0
Broadcast Address:         255.255.255.255
Host Route Propagation:    When host connected
```

ip rip routes
Displays information pertaining to the routing table(s) that are maintained by the IP RIP protocol. The following example screen illustrates the output from this command. Following the table is an explanation of the fields displayed for each route.

```
[System Name]> IP RIP ROUTES

Active Routes
Destination      Subnet-Mask      Next Hop        Mtr P 1/2 TAge
-------------------------------------------------------------------
3.2.0.0          255.255.0.0      0.0.0.0         4   A 1/1 A30
3.3.0.0          255.255.0.0      0.0.0.0         4   A 1/1 A30
192.168.5.0     255.255.255.0    0.0.0.0          0   A 1/1 SN/A
4.4.4.1          255.255.255.255 0.0.0.0          0   A 1/1 HN/A

Inactive Routes
Destination      Subnet-Mask      Next Hop        Mtr P 1/2 TAge
-------------------------------------------------------------------
4.0.0.0          255.0.0.0        0.0.0.0          0 H 0/1 SN/A
```

`Destination`
The route destination. This destination may be a network number, a subnet address, or a host address.

`Subnet-Mask`
The mask used for the destination.

`Next Hop`
The IP address or interface name (for unnumbered interfaces) of the router that is the gateway for the route.

`Mtr`
The cost of using this route (usually the number of hops to the destination).

`P`
The propagation flag, where
- `A` = Always propagate
- `N` = Do not propagate
- `H` = Propagate when Next Hop Device Connected

`1/2`
RIP Version 1/Version 2 visibility flags determine whether or not this route is visible when send the route using RIP 1 or RIP 2, where
- `0` = Invisible
- `1` = Visible

`T`
The type of route, where
- `A` = Active Route, learned via RIP on a LAN interface
- `P` = Permanent Route, learned via RIP on a WAN interface
- `S` = Static Route, learned via IP Routing Table
- `H` = Host Route, created when an IP Host Device is connected

`Age`
The time since the last update was received.

ip rip send

Used to send the IP RIP update messages to a particular interface on demand. The example screen below demonstrates how you use this command.

```
[System Name]> ip rip send 2.2.2.2

Sending IP RIP Update Message to Network 2.0.0.0
```

ip rip stats

Displays global RIP statistics and also statistics for each configured RIP interface. Refer to *RIP Statistics*, for a list of available statistics and their definitions.

ip route

Displays the current routing table. The meaning of each displayed field for a route entry is as follows:

`Destination`
IP address for the destination network or host.

`Subnet-Mask`
Subnet mask value for the destination network or host. A value of 255.255.255.255 indicates that this entry is for a specific IP host.

`Next Hop`
IP address or device name for the next hop router that provides access to the destination network or the host.

`Metric`
Hop count to the destination network or the host.

`T/P (Type/Protocol)`

`Type`
The destination type is "R" for a remote network or host, and "L" for a locally connected network or host.

`Protocol`
The mechanism used to determine the route. "L" is for local, "I" is icmp, and "R" is for RIP.

`TTL`
Time to Live for this route entry in seconds. This entry will expire after the specified number of seconds. A value of 999 implies that the entry will not expire.

`IF`
The interface Id.

`Age`
The age of the route in seconds.

ip route <IP address>

Displays the routing information for the indicated device. The meaning of each displayed field for a route entry is included in the above *ip route* command explanation.

ip stats
Displays the current IP related statistics. Refer to *IP Statistics*, for a list of available statistics and their definitions.

IPX ROUTING COMMANDS

IPX routing must be enabled before these commands can be used.

The following commands are used to display IPX routing information:

ipx ipxwan clear
Clears IPXWAN statistics.

ipx ipxwan stats (device)
Displays system-level IPXWAN statistics when device name not specified:

```
IPXWAN Statistics

Timer Request          =              Timer Response         =
Information Request    =              Information Response   =
Thruput Request        =              Thruput Response       =
Delay Request          =              Delay Response         =
NACK Sent              =              NACK Received          =
Bad Packets            =
```

Displays Negotiation Parameters when device name specified and connected:

```
WAN Statistics for device “xxxx”

Negotiation Parameters:

IPX Network Address =       IPX Node Number =
Telebit Compression =       Protocol        =
WAN Link Delay =
```

ipx diag <host ipx address> [timeout]
Tests device connectivity to specified IPX host by sending out a diag packet. If connection is up, host sends a message in response to this packet to confirm receipt. The parameters for this command are:

`host ipx address`
IPX address for the host, in <network number>:<node number> format. The network number is a hexadecimal number up to eight digits in length. The node number is the host’s MAC address. For example, if the assigned network number of “AAAA,” and the host has a MAC address of 40AA68965439. For this example, you would enter “AAAA:40AA68965439” for the host IPX address.

`timeout`
Optional parameter that indicates the number of seconds to wait for a reply. The valid range for the time out value is 1 to 60 seconds. The default value is 10.

Note: The *ipx diag* and the *ipx ping* commands both test device connectivity (although both send back different types of responses). However, due to the variety of vendors and equipment available to networks, one command may work with a particular vendor or file server, while the other may not. If you are not experiencing success with *ipx diag*, try *ipx ping*, and vice versa.

`ipx ping <host ipx address>`

Tests connectivity to the specified IPX device by sending out a data packet (echo message). If connection is up, device responds with an echo reply.

`host ipx address`

IPX address for the host, in <network number>:<node number> format. The network number is a hexadecimal number up to eight digits in length. The node number is the host's MAC address. For example, if the assigned network number of "AAAA," and the host has a MAC address of 40AA68965439. For this example, you would enter "AAAA:40AA68965439" for the host IPX address.

Note: The *ipx ping* and the *ipx diag* commands both test device connectivity (although both send back different types of responses). However, due to the variety of vendors and equipment available to networks, one command may work with a particular vendor or file server, while the other may not. If you are not experiencing success with *ipx ping*, try *ipx diag*, and vice versa.

`ipx rip stats`

Displays the IPX RIP statistics. Refer to *IPX RIP Statistics*, for a list of available statistics and their definitions.

`ipx route`

Displays the current routing table for the system, including static and learned routes.

`ipx route stats`

Displays routing table statistics, including maximum number of routes configured, and number of currently-available routes. Refer to *IPX Route Statistics*.

`ipx service`

Displays the current routes to IPX services for the system, including static and learned routes.

`ipx service stats`

Displays the current service table statistics, including the maximum number of services this router is configured to handle, and the number of currently-available services. Refer to *IPX Service Statistics*.

`ipx sap stats`

Displays the IPX SAP statistics. Refer to *IPX SAP Statistics*, for a list of available statistics and their definitions.

`ipx spoof stats`

Displays the IPX spoofing statistics. The IPX spoofing statistics displayed are self-explanatory.

`ipx stats`

Displays the IPX statistics. Refer to *IPX General Statistics*, for a list of available statistics and their definitions.

ipx trigreq [device]

Generates a triggered RIP / SAP update request to the specified device. You may use this command to initiate an update request to synchronize with the routing database of a particular WAN device.

ipx trigrip stats

Displays the triggered RIP statistics. Refer to *IPX Triggered RIP Statistics*.

ipx trigsap stats

Displays the triggered SAP statistics. Refer to *IPX Triggered SAP Statistics.*

ISDN USAGE COMMANDS

The following commands are used to display and clear ISDN B-channel monitoring information.

isdn usage

Displays the following ISDN B-channel monitoring information:

- The number of ISDN B-channels available.
- The number of ISDN B-channels in use.
- The high-water mark for the number of ISDN B-channels in use.
- The value which the number of ISDN B-channels in use must meet or exceed in order to cause an isdnUsageHigh SNMP trap to be generated by the system.
- The enabled status for the generation of the ISDN usage traps (isdnUsageHigh and isdnUsageNormal).
- The elapsed time since the monitoring of the high-water mark began.

This information can help you determine if additional lines and / or systems are necessary. For example, the high water mark could be compared to the number of ISDN B channels available, taking into consideration the elapsed time.

An example output from this command is as follows:

```
[System Name]> isdn usage

number of ISDN B channels available:  6
number of ISDN B channels in use:     3
high water mark:                      5
isdnBChanUsage trap threshold:        5
generation of ISDN usage traps:       enabled
elapsed time:                         3 days, 4 hrs, 12 min, 38 sec
```

isdn usage clear

Clears the B-channel high-water mark and elapsed time values. The purpose of this command is to allow the user to reset the high-water mark to coincide with changes to the system and / or the network or so that the user can monitor the high-water mark over desired time periods.

LAN COMMANDS

The following commands are used to display current system LAN diagnostic information:

lan stats
Displays the current LAN packet forwarding statistics, including the number of frames received and transmitted from LAN and WAN connections. Refer to *LAN Statistics*, for a list of available statistics and their definitions.

lan stat clear
Clears the current LAN packet forwarding statistics.

lan test
Transmits a test message onto the LAN and test for proper LAN connections. If the transmit is successful, the following message will be displayed:
`LAN port <port #> Transmit was successful`
If the transmit fails, refer to the section titled *LAN Attachment* to determine the reason for the failure.

PACKET CAPTURE COMMANDS

In many applications, it is often desirable to monitor incoming LAN data. The *pkt* commands will allow you to capture, display, save, and load bridged or routed data packets.

You must configure the terminal setting the same for Telnet and the terminal emulation package. To do this, use the *term set* command.

Note: Packet capture commands are available for both local and remote (Telnet) connections.

The following diagnostic packet commands are available:

pkt [on/off]
Enables or disables the Packet Capture feature.

pkt capture [all/idle/reqd/pend/actv/none]
Specifies which packets will be captured by the Packet Capture feature. A definition of each possible parameter follows.

all
All packets will be captured.

none
No packets will be captured.

reqd
Only packets causing a connection to be requested will be captured.

pend
Only packets received while a requested connection is pending will be captured.

idle
Only packets not causing a connection to be requested will be captured. This could be caused by the destination site not being in the Initiate Connection List, or by the route not being in the IP Routing Table.

The *pkt capture* command allows multiple connection modes to be specified on a single command line. For example, the command:

pkt capture reqd pend

captures only packets that cause a connection to be requested and packets that were received before the connection became active.

pkt load <filename>
Loads previously saved Packet Capture file into memory.

pkt save <filename>
Saves captured packets to a disk file. Full path names are allowed, for example: A:MYPKT.DAT.

pkt display
Displays captured packets that have been collected via *pkt on* or via *pkt load*. Note that this command is not supported for a Telnet session.

The following is an example *pkt display* screen:

```
Num   Time(mSEC) Len   Dest Addr              Source Addr             Type Conn

0001 0000000000 0064 00004440259C          02608C4C0EAD           8137 PEND
0002 0000000000 0064 00004440259C          02608C4C0EAD           8137 PEND
0003 0000000000 0064 00AA00302D25          02608C4C0EAD           8137 PEND
0004 0000000000 0064 00AA00302D25          02608C4C0EAD           8137 PEND
0005 0000001980 0064 00004440259C          02608C4C0EAD           8137 PEND
0006 0000001980 0064 00004440259C          02608C4C0EAD           8137 PEND
0007 0000001980 0064 00AA00302D25          02608C4C0EAD           8137 PEND
0008 0000001980 0064 00AA00302D25          02608C4C0EAD           8137 PEND
0009 0000003190 0028 001.001.001.001       001.001.001.001        IP    ACTV
0010 0000003190 0028 001.001.001.001       001.001.001.001        IP    ACTV
0011 0000003960 0064 00004440259C          02608C4C0EAD           8137 PEND
0012 0000003960 0064 00004440259C          02608C4C0EAD           8137 PEND
0013 0000003960 0064 00AA00302D25          02608C4C0EAD           8137 PEND
0014 0000003960 0064 00AA00302D25          02608C4C0EAD           8137 PEND
0015 0000004670 0064 FFFFFFFFFFFF          02608C4C0EAD           8137 PEND
0016 0000004670 0064 FFFFFFFFFFFF          02608C4C0EAD           8137 PEND



                    Hit <ESC> to Exit or <F1> for Help
```

It is possible to display packet details for a specific packet. To do so, use the keyboard's arrow keys to move the cursor to the desired packet number (on the "pkt display" screen); then press <return> to display detailed information for that packet. The following screens are example packet detail screens for various packet types.

NOVELL NetWare® Packet Detail Screen (Bridged Packet)

```
Packet Number      Received at Time     Packet Length
      0015             0000004670 mSEC        0064
 Destination Address    Source Address
     FFFFFFFFFFFF          02608C4C0EAD
 EtherNet Type is 8137,   Novell IPX
 Check Sum   Packet Length   Packet Type   Transport Ctl
    FFFF        0x0028         00,???          00
                  Network          Node       Socket
 Destination    0000AAA1      FFFFFFFFFFFF    0453 RIP
 Source         0000AAA1      02608C4C0EAD    0453 RIP

 Routing Information Protocol Socket Header

00 02 00 00 FF FD 00 01 00 02                    ..........


                Hit Escape to EXIT Packet Details
```

Banyan Vines Packet Detail Screen (Bridged Packet)

```
Packet Number      Received at Time     Packet Length
      0021             0000022190 mSEC        0060
 Destination Address            Source Address
     FFFFFFFFFFFF                 02608C9BED38
 EtherNet Type is 0BAD,   VINES IP
 Check Sum        Packet Length       Protocol Type
    D75D             0x001A              04, ARP
 Transport Control        Hop Count
        0                      0
 Dest Network Dest SubNet   Source Network Source SubNet
   FFFFFFFF       FFFF          00000000         0x0000

 Packet Type     Network Number      Subnetwork Number
     Query           126697007              0x9183


                    Hit Escape to EXIT Packet Details
```

IP Datagram Detail Screen (Routed Datagram)

```
Packet Number      Received at Time     Packet Length
      0009             0000003190 mSEC        0028
 Destination Address    Source Address
     001.001.001.001       001.001.001.001

45 00 1C 00 01 00 00 00 40 01 76 DD 01 01 01 01    E.......@.v.....
01 01 01 01 08 00 C3 ED 34 12 00 00               ........4...




                    Hit Escape to EXIT Packet Details
```

While the “pkt display” is displayed on your monitor, you can display the following help screen by entering “**?**”:

```
ESC   - Exit Menu
‘u’   - Previous Menu
‘d’   - Next Menu
‘h’   - Top of Packet List
‘e’   - End of Packet List
Enter - Display Packet Details
‘t’   - Time Menu
‘m’   - Marks Packet as Start Time
Cursor- to select an entry

               Hit any key to exit Help
```

The time menu that is displayed when “*t*” is entered will enable you to toggle the time increment to be in either Sec (seconds), mSec (milliseconds), or tSec (deciseconds).

When the packet marking option is used, all packet times will be displayed relative to that marked packet. To mark a packet, use the arrow keys to move the cursor to the selected packet number, then press "*m*" The time for that packet will be set to 0. All packets received before that packet will have negative time values. All packets received after that marked packet will have progressively higher positive time values.

SNMP COMMANDS

When the SNMP Agent is enabled on the SmartSwitch Remote Access Module, the following command is available:

`snmp stats`
Displays the current SNMP related statistics. Refer to *SNMP Statistics*, for a list of available statistics and their definitions.

SPANNING TREE COMMANDS

Spanning Tree protocol is supported only on the two port Ethernet-2 adapter card. The Ethernet-1 adapter card does not support Spanning Tree protocol, but does have access to the “BRIDGE AGE TIME” Spanning Tree Information.

When Spanning Tree protocol is enabled on the SmartSwitch Remote Access Module, the following commands are available:

`br stpport <port #>`
Displays Spanning Tree port information for the specified port number (either “1” or “2”).

`br stpbrdg`
Displays Spanning Tree bridge information.

SPANNING TREE PORT INFORMATION

When Spanning Tree protocol is enabled on the SmartSwitch Remote Access Module, the following Spanning Tree Port Information is available for each LAN port on the system. This information is generated by issuing the *br stpport <port #>* Spanning Tree command.

`Port Priority`
The configured priority for this port.

`State`
The current state of the port. Possible values are; DISABLED, BLOCKING, LISTENING, LEARNING, and FORWARDING.

`Path Cost`
The configured path cost for this port.

`Designated Cost`
The path cost to the root bridge for this port.

`Desig Root Addr`
The MAC address for the root bridge.

`Desig Root Prior`
The bridge priority for the root bridge.

`Desig Brdg Addr`
The MAC address for the designated bridge.

`Desig Brdg Prior`
The bridge priority for the designated bridge.

`Desig Port Number`
The port number on the designated bridge.

`Desig Port Prior`
The port priority for the port on the designated bridge.

`Topology Chng Ack`
The topology change acknowledgment value to be transmitted in the next Spanning Tree message.

`Config Pending`
The flag that indicates that the system is waiting to transmit a configuration Spanning Tree message.

SPANNING TREE BRIDGE INFORMATION

When Spanning Tree protocol is enabled on the SmartSwitch Remote Access Module, the following Spanning Tree Bridge Information is available. This information is generated by issuing the *br stpbrdg* Spanning Tree command.

`Bridge Address`
The MAC address of the SmartSwitch Remote Access Module.

`Bridge Priority`
The configured priority for the SmartSwitch Remote Access Module.

`Root Address`
The MAC address of the root bridge.

`Root Priority`
The bridge priority of the root bridge.

`Root Path Cost`
The path cost to the root bridge.

`Root Port Num`
The port number on the SmartSwitch Remote Access Module that offers the lowest cost path to the root bridge. This is set to 0 if the system is the root bridge.

`Root Port Prior`
The port priority of the Root Port Number.

`Max Age`
The maximum time (in tenths of a second) allowed without receiving a Spanning Tree message from the root bridge.

`Hello Time`
The time interval (in tenths of a second) between the transmission of configuration Spanning Tree messages. This is only used when the system is the root bridge.

`Fwd Delay Time`
The time (in tenths of a second) spent in the LISTENING and LEARNING state.

`Bridge Max Age`
The configured maximum age-time for the system. This is used when the system is the root bridge.

`Brdg Hello Time`
The configured hello time interval for this system. Used when the system is the root bridge.

`Br Fwd Delay`
The configured forward delay time for the system. Used when the system is the root bridge.

`Tplgy Chng Time`
The time period (in tenths of a second) for sending configuration Spanning Tree messages that have the topology change flag set. Only used when the system is the root bridge.

`Tplgy Ch Detect`
A flag that is set to “TRUE” when the system detects a topology change.

`Topology Change`
A flag that sets the topology change flag in configuration Spanning Tree messages that are transmitted. Used when the system is the root bridge.

`Aging Time`
The time period (in tenths of a second) used by the system to age unused entries out of the address table.

`Default Age Time`
The configured aging time the system uses.

`STP Enabled`
A flag that is set to "1" if the Spanning Tree protocol is enabled.

TCP COMMANDS

TCP (Transmit Control Protocol) provides a connection-oriented reliable communication for delivery of packets to a remote or on-node device. When the IP feature is enabled, the following TCP commands are available:

`tcp conns`
Display the current TCP connection status with the following format:

`lport`
The local port number for this TCP connection.

`fhost`
The remote IP address for this TCP connection.

`fport`
The remote port number for this TCP connection.

`window (l/r)`
The current receive windows for the local and remote ends of this TCP connection.

`tstate`
The current state of this TCP connection.

`outq (s/u)`
The number of bytes that has been sent but not acknowledged yet and the number of bytes in the output queue that has not been sent on this TCP connection.

`tcp stats`
Displays the current system TCP related statistics. Refer to *TCP Statistics*, for a list of available statistics and their definitions.

TELNET COMMANDS

These commands are Telnet client console commands. These commands provide tools for you when you are using the system as a Telnet client. As a Telnet client, the SmartSwitch Remote Access Module can then be used to Telnet into another SmartSwitch Remote Access Module to perform system maintenance, for example, updating configuration information. These commands are not needed for a Telnet session as a rule, but may be beneficial for some users. For more information

regarding the system's Telnet client feature, refer to the *Telnet* section of the *Remote System Management* chapter.

telnet ?

Displays the help screen for the *telnet* command. The help screen provides the syntax for the command described below.

telnet <ip-address> [port number]

Begins a Telnet session for the Telnet host at the indicated IP address. The port number is an optional parameter that can be used to specify the destination port number. Include this parameter if you wish to connect to a port other than the default port number, 23.

telnet

The telnet command used with no arguments, as opposed to the above command, puts you in the Telnet command mode. Once you are in the Telnet command mode, the following commands are then available.

close

Used to close the current Telnet connection to a target host.

exit

Closes the current Telnet session. If a connection exists to a target host, it is gracefully closed.

open

Used to establish a Telnet session with a target host. You can enter the IP address of the target host, and optionally, the remote port number, to connect to. If no remote port number is specified, the default Telnet port is used (23). The valid range for port number is 1 to 65535. The IP address specified is verified for proper format.

If a Telnet session is successfully initiated as a result of the *open* command, a screen similar to the following will be displayed:

```
telnet>open 204.157.42.150
Trying 204.157.42.150...
Connected to 204.157.42.150.
Escape character is '^]'.
```

If an IP address (and port) are not specified on the "open" command line, you will be prompted for the target host's IP address.

send [send parameter]

Used to send special Telnet control functions to the currently connected target host. A connection must be fully established before you can send anything. If no parameters are specified on the *send* command line, the following help message is displayed:

```
[System Name]>send
 Available send commands:
    ayt      - Send "Are You There?" request to server
    break    - Send "Break" request to server.
    escape   - Send current "escape" character to server.
    synch    - Send "Synch" signal to server.
    ?        - Display this help information.
```

The possible send parameters are defined as follows:

send ayt

The *send ayt* command sends the Telnet command function for "Are You There?" to the target host. This can be used to determine whether or not the target host is still responding. The target host is not required to respond to "are you there?" requests, but if it does, you should see something like the following:

```
[System Name]>send ayt

[Yes]
```

send break

The "send break" command sends the Telnet command function for "BREAK" to the target host. This can be used to interrupt the current command in progress on the target host. For example: If the target host is currently streaming out a large directory listing, you can issue the *send break* command to terminate the directory command. Once again, this functionality is dependent upon the target host's processing of the "BREAK" control function.

send escape

The *send escape* command sends the current escape character for the Telnet session. If the connection between the local terminal and the remote server is made up of more than 1 individual Telnet connection, this command may be used to "escape" into command mode of one of the intermediate Telnet connections.

send synch

The *send synch* command sends the Telnet "SYNCH" signal (the "DM" control function as TCP urgent data) to the target host. This command may be useful when trying correct a situation where the target host appears to be in an atypical state of processing.

set

The *set* command can be used to set certain operating parameters for the current Telnet session. The format of the *set* command is *set <name> <value>*; where <*name*> is the parameter to be set, and <*value*> is what the parameter should be set equal to.

If no parameters are specified on the "set" command line (or if "set?" is entered), the following help message is displayed:

```
[System Name]>set
 Available set commands:
    escape - Character used to escape back to TELNET command mode.
    ?      - Display this help information.
```

The *set escape* command can be used to change the "escape" character for the current Telnet session. This command may be useful when a device is connected to a target host, using several different Telnet connections. By changing the escape character to a value other than the default (<CTRL>), the user can return to Telnet "command" mode for a particular session.

Typically, Telnet "escape" characters have the form '<CTRL><char>' (i.e., the CTRL key + some other key must be pressed). The <value> parameter for the "set escape" command may have any of the following values:

- <CTRL><char>, where <char> is in the range of ASCII 'A' to ASCII '_'
- <CTRL><char>, where <char> is in the range of ASCII 'a' to ASCII 'z' (note that lower case letters are converted to upper case before they are used)
- <char>, where <char> is in the range of ASCII '!' to ASCII '~'

To specify the <CTRL> key in the *set escape* command, use the '>' character. The following is an example of setting the escape character equal to '<CTRL> P':

```
[System Name]>set escape ^P
Escape character is '^P'.
```

status

The *status* command can be used to interrogate information about the current Telnet session.

toggle

The *toggle* command can be used to set various operating parameters for the current Telnet session. Currently, the only parameter available is *debug*.

If no parameters are specified on the *toggle* command line (or if *toggle ?* is entered), the following help message is displayed:

```
[System Name]>toggle
 Available toggle commands:
    debug - Turn TELNET debug mode on or off.
    ?     - Display this help information.
```

The toggle debug command allows you to turn the Telnet debug mode on or off. If the debug mode is turned on, messages beginning with "[TELNET-C]" may appear in the system log file. Most users will not find these messages helpful. If you have difficulty with the system Telnet client feature, we suggest you call your Distributor or Customer Support.

TERMINAL COMMANDS

The SmartSwitch Remote Access Module supports two terminal types: vt100 and ANSI. When a Telnet connection is established, the system attempts to negotiate the terminal type. When the negotiation fails, the system sets the terminal type to vt100.

To successfully issue the *pkt display*, *semi perm*, and *mc* commands, you must have the terminal type set identically for both the Telnet emulator and the terminal emulation. To do this, use the *term set* command.

The following commands are used to display the terminal type currently in use or to set the terminal type.

term

Displays the terminal type name.

term set <terminal type>

Allows you to set the terminal type. You may set the terminal type to either vt100 or ANSI.

TFTP COMMANDS

The TFTP feature and its commands are only available when IP routing is enabled. The TFTP feature and file access are enabled by default when the system software is installed. The following TFTP commands are available:

tftp get

Allows you to perform the "TFTP GET" operation locally from the console through the TFTP Client function. The following is an example display of a TFTP GET screen.

```
> TFTP GET

>IP Address of the Host containing the file
(<RET> to abort)? 19.233.45.33

>Enter the name of the local file to write (including the full path)?
(<RET> to abort)? \config\config.nei

>Enter the name of the remote file (including the full path)
(<RET> for same as local)? <RET>

Enter the mode (BIN [binary] or ASC [ascii])
<RET> for ascii? bin

Receiving File... Please wait
File Transfer Complete...
```

tftp kill <session Id>

Allows you to kill a TFTP session. The session Id must be included in this command. To obtain the session Id, issue the *tftp session* command which displays the TFTP session information.

tftp put

Allows you to perform the TFTP PUT operation locally from the console through the TFTP Client function. The following is an example display of a TFTP PUT screen.

```
> TFTP PUT

>IP Address of the Host to receive the file
(<RET> to abort)? 19.233.45.33

>Enter the name of the local file to send (including the full path)
(<RET> to abort)? \config\config.nei

>Enter the name for the remote file (including the full path)
(<RET> for same as local)? <RET>

Enter the mode (BIN [binary] or ASC [ascii])
<RET> for ascii? bin

Sending File... Please wait
File Transfer Complete...
```

tftp session

Displays the TFTP session information of active TFTP sessions. To get detailed information on a specific session, enter the session's Id number when prompted. You can not display the

session information for a TFTP session that has terminated. The screen below illustrates the use of this command.

```
> TFTP SESSION

Id Sess-Id Local file    Type/Mode   Bytes Xmit Retries
-------------------------------------------------------------
 1        5 temp.txt      Client/Put       12752        1
 2        6 tmp           Server/Get         423        0
 3        7 text.txt      Server/Put        8481        0

Select the ID of the TFTP Session to display or <RET> to cancel? 2

TFTP Session ID:     6
Type:                Server
Mode:                Get
Local Address:       190.5.6.8   (UDP Port: 5001)
Local File:          c:\tmp
Remote Address:      190.5.6.11 (UDP Port: 5011)
Remote File:         N/A
Transfer Mode:       netascii
Bytes Transferred:   935
Bytes Remaining:     1145723
Total Retries:       0
```

tftp stats

Displays the current TFTP related statistics. Refer to *TFTP Statistics*, for a list of available statistics and their definitions.

TRACE COMMANDS

Note: For an explanation regarding the output resulting from the family of trace commands, refer to the *Trace Messages* chapter.

The following commands are used to enable and disable trace reporting information:

trace ipxwan [on/off]

Enables or disables the IPXWAN tracing option, which tracks all packets which are received or sent out using IPXWAN protocol, and places this information in the system log. To display the log file, issue the *dr* command. This option is initially disabled.

trace [on/off]

Enable or disables the call trace information reports. If enabled, you can then view the logged call trace information by issuing the *dr* command. For details on call trace messages, refer to the chapter titled *Trace Messages*.

trace ppp [on/off]

Enables or disables the tracing of incoming and outgoing PPP packets. If enabled, you can view the trace PPP information by issuing the *dr* command.

UDP COMMANDS

UDP (User Datagram Protocol) provides a datagram mode of communication for delivery of packets to a remote or on-node device. When the system's IP operating mode is enabled, the following UDP commands are available:

udp conns
Displays the current UDP connection status.

udp stats
Displays the current system UDP statistics. Refer to *UDP Statistics*, for a list of available statistics and their definitions.

WAN COMMANDS

The following commands are used to display current system WAN diagnostic information:

wan l1p
This group of commands provide primary rate interface layer 1 information. ***wan l1p*** is the prefix for all commands in this group. The syntax and definition for each wan l1p command follows. (Note that for each command, you must include the slot number of the PRI adapter.)

wan l1p alarm display <slot #>
Displays any alarms currently being received by the primary rate layer 1. Because many incoming alarms are qualified for several seconds before being declared, this display may indicate an alarm when layer 1 has not been declared down. The following table provides the possible alarms and their meanings.

Alarm Type	*Alarm Meaning*
Loss of Signal (Red)	An all zero signal (or complete lack of signal).
Loss of Frame (Red)	A signal which does not match the configured framing mode (for example, ESF).
AIS (Blue)	An unframed all one signal.
RAI (Yellow)	A Remote Alarm Indication signal.

wan l1p error [display or clear] <slot #>
When ***display*** is used, this command displays the PRI layer 1 error counters. Refer to *Layer 1 PRI Error Statistics* for a list of available statistics and their definitions.

wan l1p loopback status <slot #>
Displays the current status of all loopbacks. (Refer to the following two "loop" commands.

wan l1p lcl_loop [disable or enable] <slot #>
Disables or enables a local loopback. When enabled, this loopback feeds the PRI adapters's transmit signal back to the PRI adapters's receive signal. It is useful in checking for problems in the PRI adapter itself.

wan l1p rem_loop [disable or enable] <slot #>

Disables or enables a remote loopback. When enabled, this loopback feeds the network's transmit back to the network's receive. This is useful for allowing switch personnel to test the entire connection from the switch to the PRI adapter and back.

wan l1p stats [display or clear] <slot #>

When *display* is used, this command displays the PRI layer 1 statistics. Two sets of statistics are provided: the specific PRI interface statistics, and layer 1 general statistics. Refer to *WAN L1P Statistics* for a list of available statistics and their definitions.

When *clear* is used, these statistics are cleared.

wan stats

Displays the current WAN statistics. Refer to *WAN Statistics* for a list of available statistics and their definitions.

SYSTEM STATISTICS

OVERVIEW

Statistics can either be generated by issuing the *ds* command to display the set of statistics known as the System Statistics, or by issuing a specific command to display statistics in a specific category.

In addition to using the *ds* command to display the system statistics, they are also automatically written to a statistics log every 30 minutes. The statistics are stored in the following location:

Directory: `\log`
File Name: `stat_log.nn`
("`nn`" is an integer that is incremented each time a new file is written.

You may display these log files using DOS commands. For example, to display the statistics log with the extension of 10, you could enter the following command at the DOS prompt:

C:\> type \log\stat_log.10 | more

Note: The log extensions are revolving numbers. When your machine first begins operating, the files will progress from the .01 extension to the .10 extension. After that time, the oldest report (.01) would be replaced with the latest report. To make sure you are viewing the log file you wish to see, issue a DOS dir command of the log directory to display the time that each log file was written to disk.

The first set of statistics, System Statistics, are arranged by function. These are:

- connectivity statistics
- call restriction statistics
- call statistics
- throughput monitoring statistics

The rest of the statistics are arranged in alphabetical order. These statistics pertain to specific features. The statistics you choose to display will depend on which system options you have enabled. These statistics provide valuable information.

CONNECTIVITY STATISTICS

You can access Network Connectivity statistics by issuing the *ds* console command.

`ISDN_Re-try`
Retry count for re-establishing the data link after it fails.

`ID_Re-try`
Retry count for exchanging identification messages with a remote SmartSwitch Remote Access Module.

`ID_Fail`
Failure count for exchanging identification messages with a remote SmartSwitch Remote Access Module.

`WAN_Reset`
Reset count for the resetting of the WAN adapters.

CALL RESTRICTION STATISTICS

The system keeps a tally of the following Call Restriction statistics. These statistics can be compared to the limits you have configured. These statistics can be displayed by issuing the *`cr stats`* or the *`ds`* command at the administration console.

`call minutes (day)`
The total call minutes that have been logged for the day.

`call minutes (month)`
The total call minutes that have been logged for the month.

`calls (day)`
The total number of calls that have been made for the day.

`calls (month)`
The total number of calls that have been made for the month.

CALL STATISTICS

You can access these statistics by issuing the *`ds`* console command.

`Initiated`
The number of switched calls initiated.

`Completed`
The number of switched call attempts that were completed successfully.

`Re-tries`
The number of switched call retries.

`NoResource`
The number of switched call requests that could not be completed because of a call resource shortage. This could be a shortage on the requesting side or the receiving side.

THROUGHPUT MONITORING STATISTICS

You can access these statistics by issuing the *`ds`* console command.

`Overload`
The number of bandwidth overload conditions.

`Underload`
The number of bandwidth underload conditions.

`Idle`
The number of idle conditions that caused the last switched connection to be disconnected.

APPLETALK STATISTICS

You may display AppleTalk protocol statistics (subdivided into six subgroups) and AppleTalk port statistics.

You can display all six subgroups of the AppleTalk protocol statistics by issuing the ***`atalk stats`*** command, or you can display the individual subgroups by adding an extra variable to the ***`atalk stats`*** command.

You can display the AppleTalk port statistics by issuing the ***`atalk port stats`*** console command. A definition of these statistics begin on page 242.

APPLETALK PROTOCOL STATISTICS

The six subgroups of AppleTalk protocol statistics are:
- AppleTalk DDP Statistics
- AppleTalk AEP Statistics
- AppleTalk RTMP Statistics
- AppleTalk ZIP Statistics
- AppleTalk NBP Statistics
- AppleTalk ATP Statistics

We include a section of available statistics and their definitions for each subgroup.

APPLETALK DATA DELIVERY PROTOCOL (DDP) STATISTICS

You can display this subgroup of AppleTalk statistics by issuing the ***`atalk stats ddp`*** console command.

`ddpOutRequests`
The total number of DDP datagrams which were supplied to DDP by local DDP clients in requests for transmission. Note that this counter does not include any datagrams counted in ddpForwRequests.

`ddpOutShorts`
The total number of short DDP datagrams which were transmitted from this system.

`ddpOutLongs`
The total number of long DDP datagrams which were transmitted from this system.

`ddpInReceives`
The total number of input datagrams received by DDP, including those received in error.

`ddpInLocalDatagrams`
The total number of input DDP datagrams for which this system was their final DDP destination.

`ddpNoPrtclHandlers`
The total number of DDP datagrams addressed to this system that were addressed to an upper layer protocol for which no protocol handler existed.

`ddpTooShortErrors`
The total number of input DDP datagrams dropped because the received data length was less than the data length specified in the DDP header or the received data length was less than the length of the expected DDP header.

`ddpTooLongErrors`
The total number of input DDP datagrams dropped because they exceeded the maximum DDP datagram size.

`ddpShortDDPErrors`
The total number of input DDP datagrams dropped because this entity was not their final destination and their type was short DDP.

`ddpChecksumErrors`
The total number of input DDP datagrams for which this DDP entity was their final destination, and which were dropped because of a checksum error.

`ddpFwdingTblOverflws`
The number of times this system attempted to add an entry to the forwarding table but failed due to overflow.

`ddpForwRequests`
The number of input datagrams for which this system was not their final DDP destination, as a result of which an attempt was made to find a route to forward them to that final destination.

`ddpOutNoRoutes`
The total number of DDP datagrams dropped because a route could not be found to their final destination.

`ddpBroadcastErrors`
The total number of input DDP datagrams dropped because this system was not their final destination and they were addressed to the link level broadcast.

`ddpHopCountErrors`
The total number of input DDP datagrams dropped because this system was not their final destination and their hop count would exceed 15.

APPLETALK ECHO PROTOCOL (AEP) STATISTICS

You can display this subgroup of AppleTalk statistics by issuing the *`atalk stats echo`* console command.

`atechoRequests`
The number of AppleTalk Echo requests received.

`atechoReplies`
The number of AppleTalk Echo replies sent.

`atechoOutRequests`
The count of AppleTalk Echo requests sent.

`atechoInReplies`
The count of AppleTalk Echo replies received.

APPLETALK ROUTING TABLE MAINTENANCE PROTOCOL (RTMP) STATISTICS

You can display this subgroup of AppleTalk statistics by issuing the ***`atalk stats rtmp`*** console command.

`rtmpInDataPkts`
A count of the number of good RTMP data packets received by this system.

`rtmpOutDataPkts`
A count of the number of RTMP packets sent by this system.

`rtmpInRequestPkts`
A count of the number of good RTMP Request packets received by this system.

`rtmpNextIREqlChanges`
A count of the number of times RTMP changes the Next Internet Router in a routing entry because the hop count advertised in a routing table was equal to the current hop count for a particular network.

`rtmpNextIRLesChanges`
A count of the number of times RTMP changes the Next Internet Router in a routing entry because the hop count advertised in a routing table was less than the current hop count for a particular network.

`rtmpRouteDeletes`
A count of the number of times RTMP deletes a route because it was aged out of the table. This can help to detect routing problems.

`rtmpRoutingTblOvflws`
The number of times RTMP attempted to add a route to the RTMP table but failed due to lack of space.

APPLETALK ZONE INFORMATION PROTOCOL (ZIP) STATISTICS

You can display this subgroup of AppleTalk statistics by issuing the ***`atalk stats zip`*** console command.

`zipInZipQueries`
The number of ZIP Queries received by this system.

`zipInZipReplies`
The number of ZIP Replies received by this system.

`zipInZipExtReplies`
The number of ZIP Extended Replies received by this system.

`zip ZoneConflctErrors`
The number of times a conflict has been detected between this entity's zone information and another system's zone information.

`zipInObsoletes`
The number of ZIP Takedown or ZIP Bringup packets received by this system. Note that as the ZIP Takedown and ZIP Bringup packets have been obsoleted, the receipt of one of these packets indicates that a node sent it in error.

APPLETALK NAME BINDING PROTOCOL (NBP) STATISTICS

You can display this subgroup of AppleTalk statistics by issuing the ***`atalk stats nbp`*** console command.

`nbpInLookUpRequests`
The number of NBP LookUp Requests received.

`nbpInLookUpReplies`
The number of NBP LookUp Replies received.

`nbpInBroadcastReqs`
The number of NBP Broadcast Requests received.

`nbpInforwardRequests`
The number of NBP Broadcast Requests received.

`nbpOutLookUpReplies`
The number of NBP LookUp Replies sent.

`nbpRegistrationFails`
The number of times this node experienced a failure in attempting to register an NBP system.

`nbpInErrors`
The number of NBP packets received by this system that were rejected for any error.

APPLETALK TRANSACTION PROTOCOL (ATP) STATISTICS

You can display this subgroup of AppleTalk statistics by issuing the ***`atalk stats atp`*** console command.

`atpInPkts`
The number of ATP packets received by this entity.

`atpTRequestRextmis`
The number of times that a timeout occurred and a Transaction Request packet needed to be retransmitted by this host.

`atpReleaseTmExpCnts`
The number of times the release timer expired, as a result of which a Request Control Block had to be deleted.

`atpRetryCntExceeds`
The number of times the retry count was exceeded, and an error was returned to the client of ATP.

APPLETALK PORT STATISTICS

You can display the AppleTalk port statistics by issuing the *`atalk port stats`* console command.

`portInPackets`
The number of AppleTalk packets received on this port by this system.

`portOutPackets`
The number of AppleTalk packets sent out on this port by this system.

`zipInGetNetInfos`
The number of ZIP GetNetInfo packets received on this port by this system.

`zipOutGetNetInfos`
The number of ZIP GetNetInfo packets sent out this port by this system.

`zipInGetNetInfoReplies`
The number of ZIP GetNetInfo Reply packets received on this port by this system.

`zipOutGetNetInfoReplies`
The number of ZIP GetNetInfo Reply packets sent out this port by this system.

`zipZoneInInvalids`
The number of times this system has received a ZIP GetNetInfo Reply with the zone invalid bit set because the corresponding GetNetInfo Request had an invalid zone name.

`zipZoneOutInvalids`
The number of times this system has sent a ZIP GetNetInfo Reply with the zone invalid bit set in response to a GetNetInfo Request with an invalid zone name.

`zipAddressInvalids`
The number of times this system had to broadcast a ZIP GetNetInfo Reply because the GetNetInfo Request had an invalid address.

`zipInErrors`
The number of ZIP packets received by this system that were rejected for any error.

BRIDGE STATISTICS

The system collects bridge statistics for each LAN port and for WAN connections. These bridge statistics include information on the number of frames received, forwarded, discarded or transmitted. If the system is configured for two LAN ports, there is a line of counters for each LAN port. However, the WAN counters are totaled for all WAN ports.

Display bridge statistics by issuing the `br stats` command at the administration console:

`Received`
Number of frames received from a LAN port or WAN connection.

`Forwarded`
Number of frames received from LAN port 1 or LAN port 2 or all WAN ports and processed for transmission to the proper networks. Discarded frames are not forwarded for transmission.

`Discarded`
Number frames received and then discarded (i.e., not forwarded to another LAN port or WAN connection).

`Transmit`
Number of frames sent out through LAN port 1 or LAN port 2 or all WAN ports to connected networks.

Note: *Forward* refers to the passing of a *received* frame from one port to another within the SmartSwitch Remote Access Module. A frame can be received on any port (LAN or WAN) and forwarded to any other port, unless it is *discarded*. A forwarded frame is one which is not deliberately discarded (for example, via filters) by the SmartSwitch Remote Access Module. Once the frame gets to the new port, it is usually *transmitted*. However, it may not be transmitted, such as when a packet is forwarded to a WAN port, but no connection is up on that port.

COMPRESSION STATISTICS

The system collects the following compression statistics for each active compression connection. These statistics can be displayed by issuing the `cmp stats` or the `cmp stats <device name>` command at the administration console. The `cmp stats` command will display the compression statistics for all active connections. The `cmp stats <device name>` command will display the compression statistics for the specified device. Note that the device name is case sensitive.

Note: When using PPP, it is possible that CCP can open with no agreed upon compression algorithm in one or both directions. In such cases, the connection is considered to be running with compression, and will consequently be picked up by the CMP command. However, the ratios and counters for the direction(s) without an actual compression algorithm negotiated will not indicate any effective compression or decompression.

COMPRESSION RELATED STATISTICS

`cmp ratio`
The number of uncompressed bytes divided by the number of compressed bytes.

`uncmp Kbytes`
The total number of uncompressed kilobytes received.

`cmp Kbytes`
The total number of compressed kilobytes sent.

`total cmp reset count`
The total number of compression resets (peer and System sent resets).

`peer sent resets`
The number of compression resets sent from peer devices.

`system sent resets`
The number of decompression resets sent from the System.

`dropped pkts`
The number of dropped packets that could not be queued.

DECOMPRESSION RELATED STATISTICS

`dmp ratio`
The number of decompressed bytes divided by the number of compressed bytes.

`dmp Kbytes`
The total number of decompressed kilobytes sent.

`cmp Kbytes`
The total number of compressed kilobytes sent.

`total dmp reset count`
The total number of decompressed resets (peer and System sent resets).

`peer sent resets`
The number of decompression resets sent from peer devices.

`system sent resets`
The number of decompression resets sent from the System.

`dropped pkts`
The number of dropped packets that could not be queued.

`fcs errors`
The number of frame checksum errors.

DIGITAL MODEM STATISTICS

If you are using a Digital Modem, you can access the following statistics by using the *modem stats* command:

`pkts rcvd`
Total number of packets received over the modem connection.

`pkts xmit`
Total number of packets transmitted over the modem connection.

`fcs errors`
Total number of HDLC frames discarded because of Frame Checksum (FCS) errors.

LAN STATISTICS

You can access LAN statistics by issuing the *lan stats* console command.

`pkts rcvd`
The total number of packets received on the LAN port.

`rcv overruns`
The number of frames known to be lost because the local system bus was not available. If the traffic problem persists for more than one frame, the frames that follow the first are also lost; however, because there is no lost frame indicator they are not counted.

`crc errors`
The number of aligned frames discarded because of a CRC error.

`align errors`
The number of frames that are both misaligned and contain a CRC error.

`resource errors`
The number of good frames discarded because there were no resources available.

`pkts xmit`
The number of packets transmitted on the LAN port.

`xmit errors`
The number of packets transmitted with errors on the LAN port.

IP STATISTICS

You can access IP statistics by using the *ip stats* console command. These statistics are parts of the IP Group and the ICMP Group MIB variables that are defined in RFC-1213:MIB-II.

IP GROUP STATISTICS

`ipForwarding`
The indication of whether the system is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this SmartSwitch Remote Access Module. IP gateways forward datagrams, IP hosts do not (except those source-routed via the host).

`ipDefaultTTL`
The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this system, whenever a TTL value is not supplied by the transport layer protocol.

`ipInReceives`
The total number of input datagrams received from interfaces, including those received in error.

`ipInHdrErrors`
The number of input datagrams discarded due to errors in their IP headers. Possible errors include bad checksums, version number mismatches, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

`ipInAddrErrors`
The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this system. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For systems that are not IP Gateways, and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

`ipForwDatagrams`
The number of input datagrams for which this system was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In systems that do not act as IP Gateways, this counter will include only those packets that were Source-Routed via this system, and the Source-Route option processing was successful.

`ipInUnknownProtos`
The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

`ipInDiscards`
The number of input IP datagrams for which no problems were encountered that would prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

`ipInDelivers`
The total number of input datagrams successfully delivered to IP device-protocols (including ICMP).

`ipOutRequests`
The total number of IP datagrams which local IP device-protocols (including ICMP) supplied to IP in requests for transmission.

`ipOutDiscards`
The number of output IP datagrams for which no problem was encountered that would prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space).

Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.

`ipOutNoRoutes`
The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams that meet this “no-route” criterion. Note that this includes any datagrams that a host cannot route because all of its default gateways are down.

`ipReasmTimeout`
The maximum number of seconds that received fragments are held while they are awaiting reassembly at this system.

`ipReasmReqds`
The number of IP fragments received which needed to be reassembled at this system.

`ipReasmOKs`
The number of IP datagrams successfully reassembled.

`ipReasmFails`
The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

`ipFragOKs`
The number of IP datagrams that have been successfully fragmented at this system.

`ipFragFails`
The number of IP datagrams that have been discarded because they needed to be fragmented at this system but could not be, for example, because their “Don't Fragment” flag was set.

`ipFragCreates`
The number of IP datagram fragments that have been generated as a result of fragmentation at this system.

ICMP GROUP STATISTICS

`icmpInMsgs`
The total number of ICMP messages that the system received. Note that this counter includes all those counted by icmpInErrors.

`icmpInErrors`
The number of ICMP messages that the system received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).

`icmpInDestUnreachs`
The number of ICMP Destination Unreachable messages received.

`icmpInTimeExcds`
The number of ICMP Time Exceeded messages received.

`icmpInParmProbs`
The number of ICMP Parameter Problem messages received.

`icmpInSrcQuenchs`
The number of ICMP Source Quench messages received.

`icmpInRedirects`
The number of ICMP Redirect messages received.

`icmpInEchos`
The number of ICMP Echo (request) messages received.

`icmpInEchoReps`
The number of ICMP Echo Reply messages received.

`icmpInTimestamps`
The number of ICMP Timestamp (request) messages received.

`icmpInTimestampReps`
The number of ICMP Timestamp Reply messages received.

`icmpInAddrMasks`
The number of ICMP Address Mask Request messages received.

`icmpInAddrMaskReps`
The number of ICMP Address Mask Reply messages received.

`icmpOutMsgs`
The total number of ICMP messages that this system attempted to send. Note that this counter includes all those counted by icmpOutErrors.

`icmpOutErrors`
The number of ICMP messages that this system did not send due to problems discovered within ICMP, such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no error types that contribute to this counter's value.

`icmpOutDestUnreachs`
The number of ICMP Destination Unreachable messages sent.

`icmpOutTimeExcds`
The number of ICMP Time Exceeded messages sent.

`icmpOutParmProbs`
The number of ICMP Parameter Problem messages sent.

`icmpOutSrcQuenchs`
The number of ICMP Source Quench messages sent.

`icmpOutRedirects`
The number of ICMP Redirect messages sent. For a host, this will always be zero, since hosts do not send redirects.

`icmpOutEchos`
The number of ICMP Echo (request) messages sent.

`icmpOutEchoReps`
The number of ICMP Echo Reply messages sent.

`icmpOutTimestamps`
The number of ICMP Timestamp (request) messages sent.

`icmpOutTimestampReps`
The number of ICMP Timestamp Reply messages sent.

`icmpOutAddrMasks`
The number of ICMP Address Mask Request messages sent.

`icmpOutAddrMaskReps`
The number of ICMP Address Mask Reply messages sent.

IPX STATISTICS

You can access the following types of IPX statistics: general, RIP and triggered RIP, SAP and triggered SAP and IPX spoofing. The sections below provide information for each category.

IPX GENERAL STATISTICS

You can access IPX general statistics by using the *`ipx stats`* console command. IPX general statistics include basic and advanced system table statistics.

IPX BASIC SYSTEM TABLE STATISTICS

`ipxBasicSysExistState`
The validity of this entry in the IPX system table. Setting this field to off indicates that this entry may be deleted from the system table at the IPX implementation's discretion.

`ipxBasicSysNetNumber`
The network number portion of the IPX address of this system.

`ipxBasicSysName`
The readable name for this system.

`ipxBasicSysInReceives`
The total number of IPX packets received, including those received in error.

`ipxBasicSysInHdrErrors`
The number of IPX packets discarded due to errors in their headers, including any IPX packet with a size less than the minimum of 30 bytes.

`ipxBasicSysInUnknownSockets`
The number of IPX packets discarded because the destination socket was not open.

`ipxBasicSysInDiscards`
The number of IPX packets received but discarded due to reasons other than those accounted for by ipxBasicSysInHdrErrors, ipxBasicSysInUnknownSockets, ipxAdvSysInDiscards, and ipxAdvSysInCompressDiscards.

`ipxBasicSysInBadChecksums`
The number of IPX packets received with incorrect checksums.

`ipxBasicSysInDelivers`
The total number of IPX packets delivered locally including packets from local applications.

`ipxBasicSysNoRoutes`
The number of times no route to a destination was found.

`ipxBasicSysOutRequests`
The number of IPX packets supplied locally for transmission, not including any packets counted in ipxAdvForwPackets.

`ipxBasicSysOutMalformedRequests`
The number of IPX packets supplied locally that contained errors in their structure.

`ipxBasicSysOutDiscards`
The number of outgoing IPX packets discarded due to reasons other than those accounted for in ipxBasicSysOutMalformedRequests, ipxAdvSysOutFiltered and ipxAdvSysOutCompressDiscards.

`ipxBasicSysOutPackets`
The total number of IPX packets transmitted.

`ipxBasicSysConfigSockets`
The configured maximum number of IPX sockets that may be open at one time.

`ipxBasicSysOpenSocketFails`
The number of IPX socket open calls which failed.

IPX ADVANCED SYSTEM TABLE STATISTICS

`ipxAdvSysMaxPathSplits`
The maximum number of paths with equal routing metric value which this instance of the IPX may split between when forwarding packets.

`ipxAdvSysMaxHops`
The maximum number of hops a packet may take.

`ipxAdvSysInTooManyHops`
The number of IPX packets discarded due to exceeding the maximum hop count.

`ipxAdvSysInFiltered`
The number of incoming IPX packets discarded due to filtering.

`ipxAdvSysInCompressDiscards`
The number of incoming IPX packets discarded due to decompression errors.

`ipxAdvSysNETBIOSPackets`
The number of NETBIOS packets received.

`ipxAdvSysForwPackets`
The number of IPX packets forwarded.

`ipxAdvSysOutFiltered`
The number of outgoing IPX packets discarded due to filtering.

`ipxAdvSysOutCompressDiscards`
The number of outgoing IPX packets discarded due to compression errors.

`ipxAdvSysCircCount`
The number of circuits known to this instance of IPX.

`ipxAdvSysDestCount`
The number of currently reachable destinations known to this instance of IPX.

`ipxAdvSysServCount`
The number of services known to this instance of IPX.

IPX RIP STATISTICS

You can access IPX RIP statistics by using the *`ipx rip stats`* console command.

`ripInstance`
With the SmartSwitch Remote Access Module, the value of this statistic is always 1. With other products, this statistic is useful. Currently, it is not useful for the SmartSwitch Remote Access Module.

`ripIncorrectPackets`
The number of times incorrect RIP packets were received.

`ripState`
Represents the status of the IPX RIP feature: 1 = disabled, 2 = enabled.

IPX TRIGGERED RIP STATISTICS

You can access IPX triggered RIP statistics by using the *`ipx trigrip stats`* command.

trigRipUpdateRequestsSent
Number of triggered RIP update requests sent.

trigRipUpdateRequestsRcvd
Number of triggered RIP update requests received.

trigRipUpdateResponsesSent
Number of triggered RIP update responses sent.

trigRipUpdateResponsesRcvd
Number of triggered RIP update responses received.

trigRipUpdateAcksSent
Number of triggered RIP update acknowledgments sent.

trigRipUpdateAcksRcvd
Number of triggered RIP update acknowledgments received.

trigRipInputErrors
Number of Triggered RIP input message errors.

IPX ROUTE STATISTICS

You can access IPX Route statistics by using the *ipx route stats* console command.

`Static Routes`
Number of static routes configured on this router.

`Rip Routes`
Number of routes learned through RIP from other routers.

`Internal Routes`
Number of internal routes on this router. There is one for the internal network number, and two for each IPX network interface.

`Total Routes`
Total number of routes. Should be equal to the sum of Static, RIP and Internal Routes.

`Maximum Routes`
Maximum number of routes this router is configured to handle.

`Available Routes`
Number of routes currently available on this router.

`High Water Mark`
Peak number of routes this router has used.

IPX SAP STATISTICS

You can access IPX SAP statistics by using the *ipx sap stats* console command.

`sapInstance`
With the SmartSwitch Remote Access Module, the value of this statistic is always 1. With other products, this statistic is useful. Currently, it is not useful for the SmartSwitch Remote Access Module.

`sapIncorrectPackets`
The number of times incorrect SAP packets were received.

`sapState`
Represents the status of the IPX SAP feature: 1 = disabled, 2 = enabled.

IPX TRIGGERED SAP STATISTICS

You can access IPX triggered SAP statistics by using the *`ipx trigsap stats`* command.

`trigSapUpdateRequestsSent`
Number of triggered SAP update requests sent.

`trigSapUpdateRequestsRcvd`
Number of triggered SAP update requests received.

`trigSapUpdateResponsesSent`
Number of triggered SAP update responses sent.

`trigSapUpdateResponsesRcvd`
Number of triggered SAP update responses received.

`trigSapUpdateAcksSent`
Number of triggered SAP update acknowledgments sent.

`trigSapUpdateAcksRcvd`
Number of triggered SAP update acknowledgments received.

`trigSapInputErrors`
Number of Triggered SAP input message errors.

IPX SERVICE STATISTICS

You can access IPX Service statistics by using the *`ipx service stats`* console command.

`Static Services`
Number of static services configured on this router.

`Sap Services`
Number of services learned through SAP from other routers.

`Total Services`
Total number of services. Should be equal to the sum of Static and SAP services.

`Maximum Services`
Maximum number of services this router is configured to handle.

`Available Services`
Number of services currently available on this router.

`High Water Mark`
Peak number of services this router has used.

RIP STATISTICS

You can access RIP statistics by using the *ip rip stats* console command. Global RIP statistics and statistics for each configured RIP interface are included.

RIP GLOBAL STATISTICS

`GlobalRouteChanges`
The number of route changes made to the IP route database by RIP. This does not include the refresh of a route's age.

`GlobalQueries`
The number of responses sent to RIP queries from other systems.

RIP INTERFACE STATISTICS

The following set of RIP interface statistics are displayed for each configured RIP interface.

`IfStatAddress`
The IP address of this system on the indicated RIP interface. For unnumbered interfaces, the value 0.0.0.N, where the last signification 24 bits (N) is the index for the IP interface in network byte order.

`IfStatRcvBadPackets`
The number of RIP response packets received by the RIP process which were subsequently discarded for any reason. Example reasons include: a version 0 packet, or an unknown command type.

`IfStatRcvBadRoutes`
The number of routes, in valid RIP packets, which were ignored for any reason. Example reasons include: an unknown address family, or an invalid metric.

`IfStatRcvRequests`
The number of RIP messages with 'request' command code received on this interface.

`IfStatRcvResponses`
The number of RIP messages with 'response' command code received on this interface.

`IfStatSentRequests`
The number of RIP messages with 'request' command code sent on this interface.

`IfStatSentResponses`
The number of RIP messages with 'response' command code sent on this interface.

`IfStatSentUpdates`
The number of triggered RIP updates actually sent on this interface. This explicitly does NOT include full updates sent containing new information.

SNMP STATISTICS

If the SNMP Agent is enabled, you can access SNMP statistics by using the *snmp stats* command. Each of the following statistics are counters that refer to an MIB-2 SNMP group object.

`snmpInPkts`
The total number of messages delivered to the SNMP Agent from the transport service.

`snmpOutPkts`
The total number of SNMP messages that were passed from the SNMP Agent to the transport service.

`snmpInBadVersions`
The total number of SNMP messages that were delivered to the SNMP Agent and were for an unsupported SNMP version.

`snmpInBadCommunityNames`
The total number of SNMP messages delivered to the SNMP Agent that used an SNMP community name not known to said system.

`snmpInBadCommunityUses`
The total number of SNMP messages delivered to the SNMP Agent that represented an SNMP operation that was not allowed by the SNMP community named in the message.

`snmpInASNParseErrs`
The total number of ASN.1 or BER errors encountered by the SNMP Agent when decoding received SNMP messages.

`snmpInTooBigs`
The total number of SNMP PDUs that were delivered to the SNMP Agent and for which the value of the error-status field is “tooBig”.

`snmpInNoSuchNames`
The total number of SNMP PDUs that were delivered to the SNMP Agent and for which the value of the error-status field is “noSuchName”.

`snmpInBadValues`
The total number of SNMP PDUs that were delivered to the SNMP Agent and for which the value of the error-status field is “badValue”.

`snmpInReadOnlys`
The total number of valid SNMP PDUs that were delivered to the SNMP Agent and for which the value of the error-status field is “readOnly”. It should be noted that it is a protocol error to generate an SNMP PDU that contains the value “readOnly” in the error-status field, as such this object is provided as a means of detecting incorrect implementations of the SNMP.

`snmpInGenErrs`
The total number of SNMP PDUs that were delivered to the SNMP Agent and for which the value of the error-status field is “genErr”.

`snmpInTotalReqVars`
The total number of MIB objects that have been retrieved successfully by the SNMP Agent as the result of receiving valid SNMP Get-Request and Get-Next PDUs.

`snmpInTotalSetVars`
The total number of MIB objects that have been altered successfully by the SNMP Agent as the result of receiving valid SNMP Set-Request PDUs.

`snmpInGetRequests`
The total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP Agent.

`snmpInGetNexts`
The total number of SNMP Get-Next PDUs that have been accepted and processed by the SNMP Agent.

`snmpInSetRequests`
The total number of SNMP Set-Request PDUs that have been accepted and processed by the SNMP Agent.

`snmpInGetResponses`
The total number of SNMP Get-Response PDUs that have been accepted and processed by the SNMP Agent.

`snmpInTraps`
The total number of SNMP Trap PDUs that have been accepted and processed by the SNMP Agent.

`snmpOutTooBigs`
The total number of SNMP PDUs that were generated by the SNMP Agent and for which the value of the error-status field is "tooBig".

`snmpOutNoSuchNames`
The total number of SNMP PDUs that were generated by the SNMP Agent and for which the value of the error-status is "noSuchName".

`snmpOutBadValues`
The total number of SNMP PDUs that were generated by the SNMP Agent and for which the value of the error-status field is "badValue".

`snmpOutGenErrs`
The total number of SNMP PDUs that were generated by the SNMP Agent and for which the value of the error-status field is "genErr".

`snmpOutGetRequests`
The total number of SNMP Get-Request PDUs that have been generated by the SNMP Agent.

`snmpOutGetNexts`
The total number of SNMP Get-Next PDUs that have been generated by the SNMP Agent.

`snmpOutSetRequests`
The total number of SNMP Set-Request PDUs that have been generated by the SNMP Agent.

`snmpOutGetResponses`
The total number of SNMP Get-Response PDUs that have been generated by the SNMP Agent.

`snmpOutTraps`
The total number of SNMP Trap PDUs that have been generated by the SNMP Agent.

`snmpEnableAuthenTraps`
Indicates whether the SNMP agent process is permitted to generate authentication-failure traps. The value of this object overrides any configuration information. For example, it provides a means whereby all authentication-failure traps may be disabled.

TCP STATISTICS

You can access these statistics by issuing the *`tcp stats`* console command.

`tcpRtoAlgorithm`
The algorithm used to determine the timeout value used for retransmitting unacknowledged octets. This value is always equal to 4 for the Van Jacobson's algorithm.

`tcpRtoMin`
The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.

`tcpRtoMax`
The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.

`tcpMaxConn`
The limit on the total number of TCP connections the system can support.

`tcpActiveOpens`
The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

`tcpPassiveOpens`
The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

`tcpAttemptFails`
The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

`tcpEstabResets`
The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

`tcpCurrEstab`
The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT. This counter is not currently kept up to date.

`tcpInSegs`
The total number of segments received, including those received in error. This count includes segments received on currently established connections.

`tcpOutSegs`
The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

`tcpRetransSegs`
The total number of segments retransmitted (the number of tcp segments transmitted containing one or more previously transmitted octets).

`tcpInErrs`
The total number of segments received in error (for example, bad TCP checksums).

`tcpOutRsts`
The number of TCP segments sent containing the RST flag.

TFTP STATISTICS

You can access these statistics by issuing the ***`tftp stats`*** console command.

STATISTICS FOR SERVER OR REMOTE INITIATED TFTP ACTIVITY

`Successful file puts`
Displays the count of the successful puts from the remote hosts.
(Remote host uploaded a file to local system.)

`Successful file gets`
Displays the count of the successful gets from the remote hosts.
(Remote host downloaded a file from the local system.)

`Failed file puts`
Displays the count of failed puts.
(Remote host failed to upload a file to the local system.)

`Failed file gets`
Displays the count of failed gets.
(Remote host failed to download a file from the local system.)

`Total bytes put`
Displays the total number of bytes successfully put.
(Number of bytes uploaded to the local system by remote hosts.)

`Total bytes get`
Displays the total number of bytes successfully gotten.
(Number of bytes downloaded from the local system by remote hosts.)

STATISTICS FOR LOCAL OR CLIENT INITIATED TFTP ACTIVITY

`Successful file puts`
Displays the count of successful puts from the local system.
(Files uploaded from the local system to remote hosts.)

`Successful file gets`
Displays the count of successful gets to the local system.
(Files downloaded from remote hosts to the local system.)

`Failed file puts`
Displays the count of failed puts.
(Local system failed to upload a file to a remote host.)

`Failed file gets`
Displays the count of failed gets.
(Local system failed to download a file from a remote host.)

`Total bytes put`
Displays the total number of bytes successfully put.
(Number of bytes uploaded from the local system to remote hosts.)

`Total bytes get`
Displays the total number of bytes successfully gotten.
(Number of bytes downloaded from remote hosts to the local system.)

STATISTICS FOR ALL TFTP ACTIVITY

`Read Requests Sent`
Displays the total number of Read Requests sent.

`Read Requests Received`
Displays the total number of Read Requests received.

`Write Requests Sent`
Displays the total number of Write Requests sent.

`Write Requests Received`
Displays the total number of Write Requests received.

`Data Packets Sent`
Displays the total number of Data Packets sent.

`Data Packets Received`
Displays the total number of Data Packets received.

`Error Packets Sent`
Displays the total number of Error Packets sent.

`Error Packets Received`
Displays the total number of Error Packets received.

`ACK Packets Sent`
Displays the total number of ACK Packets sent.

`ACK Packets Received`
Displays the total number of ACK packets received.

`TFTP Sessions Opened`
Displays the total number of TFTP Sessions that have been opened.

`TFTP Sessions Closed`
Displays the total number of TFTP Sessions that have been closed.

`TFTP Sessions still open`
Displays the total number of TFTP Sessions that are still open.

UDP STATISTICS

If the IP operating mode is enabled, you can access the following UDP statistics by using the *`udp stats`* command:

`udpInDatagrams`
The total number of UDP datagrams delivered to UDP devices.

`udpInErrors`
The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

`udpNoPorts`
The total number of received UDP datagrams for which there was no application at the destination port.

`udpOutDatagrams`
The total number of UDP datagrams sent from this system.

WAN L1P STATISTICS

You can access WAN L1P statistics by issuing the *`wan l1p stats display <slot #>`* console command. These statistics are divided into the following groups of statistics: PRI S/T (T1/E1) interface statistics, error statistics, and layer 1 general statistics. These groups are defined below.

PRI S/T (T1/E1) INTERFACE STATISTICS

`Layer 1 Up`
The number of times layer 1 has reported itself up to the upper ISDN layers.

`Layer 1 Down`
The number of times layer 1 has reported itself down to the upper ISDN layers.

`L1 Deactivates`
The number of times the upper ISDN layers requested layer 1 to deactivate.

`Loss of Frame (RED)`
The number of times layer 1 has detected a qualified loss of frame condition; excluding AIS (alarm indication signal).

`Loss of Signal (RED)`
The number of times layer 1 has detected an all zero signal (or complete lack of signal).

`AIS (Blue)`
The number of times layer 1 has detected a qualified unframed all ones signal.

`RAI (Yellow)`
The number of times layer 1 has detected a qualified RAI (remote alarm indication) signal.

LAYER 1 PRI ERROR STATISTICS

Note: Layer 1 PRI error statistics apply to the line connected to the indicated slot.

`Bipolar Violations`
The number or times there has been either a mismatch between encoding types (B8ZS not selected) or line noise.

`ESF CRC Errors`
The number of Cyclic Redundancy Check (CRC) errors in the PRI framing format (ESF framing only).

`Framing Bit Errors`
The number of errors in the framing bits of the PRI layer 1 framing format.

`Recv Negative Slips`
The Number of PRI frames lost due to timing problems in the negative direction.

`Global Parity Errors`
The number of parity errors seen across all transmit and receive channels.

`Recv Positive Slips`
The number of PRI frames lost due to timing problems in the positive direction.

`Recv Parity Errors`
The number of receive parity errors.

`Xmit Slips`
The number of times an error has occurred in the host clock system. If the wander of the transmit route clock is too great, data transmission errors will occur.

`Xmit Parity Errors`
The number of transmit parity errors.

LAYER 1 GENERAL STATISTICS

Note: Layer 1 general statistics apply to the indicated slot.

`Interrupts`
The number of hardware interrupts received from the layer 1 hardware device.

`Forced Resynchs`
The number of times layer 1 has attempted to manually synchronize to the incoming signal.

`Unknown Events`
If this counter is ever non-zero, call Customer Support Personnel.

`Unused Events`
If this counter is ever non-zero, call Customer Support Personnel.

`Unknown Mail`
If this counter is ever non-zero, call Customer Support Personnel.

`Wrong State`
If this counter is ever non-zero, call Customer Support Personnel.

WAN STATISTICS

You can access WAN statistics by issuing the *`wan stats`* console command.

`data link up`
A counter that is incremented every time a data link comes up.

`data link down`
A counter that is incremented each time a data link goes down.

`switched call initiated`
A counter that is incremented for each attempt to make a switched call.

`switched call completed`
A counter that is incremented each time a switched call successfully completes and passes identification.

`switched call retry`
A counter that is incremented for each retry of an original switched call attempt.

`switched call not possible`
A counter that is incremented each time a switched call needs to be made to a site and it is not possible.

`connection request failure`
A counter that is incremented each time a connection is requested and no response has been received after a connection request failure period of time.

`rcv fail`
A counter that is incremented each time an incoming connection is accepted and no response has been received after a connection receive failure period of time.

`wan board recover`
A counter that is incremented each time a WAN board is restarted after it originally comes up.

`call minutes (day)`
The total call minutes that have been logged for the day.

`call minutes (month)`
The total call minutes that have been logged for the month.

`calls (day)`
The total number of calls that have been made for the day.

`calls (month)`
The total number of calls that have been made for the month.

ROUTINE MAINTENANCE

OVERVIEW

The information in this chapter provides instructions for performing routing maintenance on the SmartSwitch Remote Access Module. The information falls into the following categories:

- installing / upgrading system software
- performing a configuration backup and restore
- obtaining system custom information

INSTALLING/UPGRADING SYSTEM SOFTWARE

System software is delivered on 3.5" high-density diskettes. For details regarding your specific software version, view the System Release Notes by issuing the `list rel_notes.txt` command. For installation and / or upgrade details, refer to *Upgrading System Software*.

CONFIGURATION BACKUP AND RESTORE

After making configuration changes, back up the new configuration, either to diskette or network management station. To accomplish this, use TFTP to copy the configuration data (\system*.nei) from one machine to another. For more information on TFTP, refer to the *Remote Management* chapter.

To restore a configuration, use TFTP to transfer the configuration files back to the system. Then restart the system for the new configuration to take effect.

OBTAINING SYSTEM CUSTOM INFORMATION

If diskettes are included with your system, the labels affixed to the System Diskettes specify customized information for that copy of the system software, which may include: Version, Serial Number, Variant, Release and Options. Once this software is installed on the system, it is possible to obtain this information from the Administration Console when the system is running by issuing the `ver` command at the system prompt. The customized information for the system software will then be displayed.

APPENDICES

The *User's Guide* includes the following appendices:

- *Getting Assistance*
  Includes a System Problem Report you can use to inform us of any difficulties you have with our products.

- *System Commands*
  A table that lists all system administration commands (including both Administrative and Guest commands).

- *Cause Codes*
  A table that provides Q.931 cause codes and their corresponding meanings. Cause codes may appear in Call Trace Messages.

GETTING ASSISTANCE

REPORTING PROBLEMS

For a fast response, please take the time to fill out the System Problem Report to inform us of any difficulties you have with our products. A copy of this report can be found at the end of this chapter. This report provides us with important information to diagnose and respond to your questions. Please pay special attention to the following areas:

FAX Header
The System Problem Report has been designed as a FAX form. Please fill in all information in this area before you FAX the report to Cabletron Systems. If you plan to mail the System Problem Report, please fill in the company information in this section for reference information.

Software
Please fill in the following sections:
- Release, Issue, and Version (From the VERsion command.)

Hardware
Select the Platform and resources that you are using.

Problem
Please fill in the following sections:
- Type (Software, Hardware, Unknown.)
- Occurrence (Reproducible, Intermittent, Single Occurrence.)
- Original Number (This field is for your use. Enter your problem tracking number, if desired, for future reference.)
- Description (Briefly describe the problem you are experiencing.)

Description (including sequence of events):
Briefly describe the problem you are experiencing. As best you can, describe the events or conditions that led to the problem you are experiencing.

Please send the System Problem Report form and any extra information (for example, line traces, system reports, and configuration files) that you have.

CONTACTING CABLETRON SYSTEMS

You can call us directly at:

Phone: (603) 332-9400
FAX: (603) 337-3075 fax

or, you can send email to us at:

support@ctron.com

DATE: _____ NUMBER OF PAGES INCLUDING THIS PAGE: _____

TO: CUSTOMER SERVICE
Cabletron Systems
(603) 332-9400 PHONE
(603) 337-3075 FAX

FROM: _____
COMPANY:_____
ADDRESS: _____
_____
PHONE: _____
FAX: _____

CABLETRON SYSTEMS
SYSTEM PROBLEM REPORT

SOFTWARE

Release: _____ Issue: _____ Version: _____

HARDWARE

Platform		Resources	
__ CSX154	__ 9W006-200	__ Ethernet-1	__ BRI-4
__ CSX155	__ 9W006-400	__ Ethernet-2	__ V.35
__ CSX1000	__ 9W006-220	__ PRI-8	__ RS232
__ CSX1200	__ 9W007-200	__ PRI- 23	__ DM8
__ CSX5500	__ 9W007-400	__ PRI- 23/30	__ DM24
__ CSX6000	__ 9W007-220	__ Expander	__ DM24+
__ CSX7000		__ BRI-1	__ DM30

PROBLEM

Type	Occurrence
__ Hardware	__ Reproducible
__ Software	__ Intermittent
__ Unknown	__ Single Occurrence

DESCRIPTION (including sequence of events prior to problem occurrence):

_____

_____

_____

_____

_____

_____

CABLETRON SYSTEMS USE ONLY

Control No:	Priority:	Date Received:
Resolution:		

ADMINISTRATIVE CONSOLE COMMANDS TABLE

The following table lists all system administration commands. Guest commands are identified in the command column.

Command	*Use*
? (GUEST)	displays help screen
atalk arp	displays the AARP cache
atalk ping <dnet>.<dnode> {timeout/dnnn] *example:* *atalk ping 1.3 30 /d200*	pings a specified device, where: dnet = destination network number (required) dnode = destination node ID (required) timeout = seconds to wait for reply (optional) nnn = data size included in ping packet (optional)
atalk port	displays AppleTalk port information
atalk port stats [clear]	displays or clears current AppleTalk port statistics
atalk route	displays AppleTalk static route information
atalk stats	displays all six groups of current AppleTalk statistics the commands below display individual group statistics
atalk stats atp	displays current AppleTalk ATP statistics
atalk stats ddp	displays current AppleTalk DDP statistics
atalk stats echo	displays current AppleTalk AEP statistics
atalk stats nbp	displays current AppleTalk NBP statistics
atalk stats rtmp	displays current AppleTalk RTMP statistics
atalk stats zip	displays current AppleTalk ZIP statistics
atalk zone	displays AppleTalk zone information
br stats	displays current packet statistics
br stats clear	clears current packet statistics
br stpbrdg	displays Spanning Tree bridge information
br stpport <port #>	displays Spanning Tree information for the specified port
call peer *<phone number> [data rate]*	calls a device at the given phone number, data rate is optional
call device <device name>	calls the specified device
cls (GUEST)	clears administration screen

Command	*Use*
cmp stats	displays the compression connection statistics for all active connections
cmp stats <device name>	displays the compression connection statistics for the specified device
cmp clear <device name>	clears all the compression statistics for the specified device
cmp clearall	clears all active connection compression statistics
cr stats	displays the call restriction statistics
cs (GUEST)	displays connected device information
date <month, day, year>	changes the date as specified
disc device <device name>	disconnects all calls to the specified device
dr (GUEST)	displays message reports
ds (GUEST)	displays system statistics
er	erases current system messages in memory
es	erases current system statistics in memory
exit (GUEST)	terminates a session
ip addrpool	displays the current IP address pool
ip arp	displays current ARP cache table
ip ping <host ip address>	sends an ICMP echo message to the specified host
ip rip interface	displays IP RIP interface information
ip rip routes	displays IP RIP routing table(s)
ip rip send	forces an IP RIP update message to be sent
ip rip stats	displays IP RIP statistics
ip route	displays the current routing table
ip route <IP address>	displays the routing information for the indicated device
ip stats	displays or resets current IP related statistics
ipconfig	allows you to change the system's default IP address
ipx diag <host>[timeout]	sends a diag packet to the specified host to confirm connectivity; timeout value optional
ipx ipxwan clear	clears IPXWAN stats
ipx ipxwan stats <device>	displays system-level or device-level statistics
ipx ping <host>	sends an ICMP echo message to the specified host

Command	*Use*
ipx rip stats	displays IPX RIP statistics
ipx route	displays the current IPX routing table
ipx route stats	displays IPX routing table statistics
ipx sap stats	displays IPX SAP statistics
ipx service	displays routes to IPX services
ipx service stats	displays current service table statistics
ipx sap stats	displays IPX SAP statistics
ipx spoof stats	displays IPX spoofing statistics
ipx stats	displays IPX statistics
ipx trigreq <device>	generates a triggered RIP/SAP update request to the specified device.
ipx trigrip stats	displays the triggered RIP statistics
ipx trigsap stats	displays the triggered SAP statistics
isdn usage	displays ISDN B-channel monitoring information
isdn usage clear	clears portion of ISDN B-channel monitoring information
lan stats	displays current LAN packet forwarding information
lan stats clear	clears current LAN packet forwarding information
lan test	tests for proper LAN connections
led status	allows you view snapshot of remote device's LED information
list [file name]	displays the indicated file useful for displaying Release Notes ("list rel_notes.txt")
logout (GUEST)	terminates a session
mc (GUEST)	displays connection monitor screen
modem add <slot# modem#>	adds a modem back to available list
modem delete <slot# modem#>	deletes a modem from available list
modem reset <slot# modem #>	resets specified modems on specified slot
modem restart <slot#>	restarts the digital modem board only
modem stats <slot# modem#>	displays modem statistics for specified modem
modem stats clear <slot # modem #>	clears modem statistics for specified modem
modem status	displays slots that have valid digital modem boards

Command	*Use*
modem upgrade <slot# modem#>	installs new modem firmware onto specified modem
modem devices <data>	displays active modem connections
neif	displays the interface table
pkt capture <connection mode>	specifies which packets will be captured by the packet capture feature (all, reqd, pend, actv, idle, or none)
pkt mac	enables the MAC address monitor display
pkt [on/off]	enables or disables the Packet Capture feature
pkt display	displays captured packets
pkt load <filename>	loads previously saved Packet Capture file into memory
pkt save <filename>	saves captured packets to a disk file
pswd (GUEST)	changes password for current access level
quit	terminates system program
restore	copies backup config files into current files
restart	restarts the system program remotely using Telnet
session	displays the current active administration sessions
session kill <session id>	terminates the active session specified by the session id
snmp stats	displays current SNMP related statistics
sp	lists each semi-permanent device and associated status
start_ne	starts or restarts system software
status (GUEST)	displays system errors and system messages
tcp conns	displays the current TCP connection status
tcp stats	displays the current system TCP statistics
telnet	puts you in the Telnet command mode see `telnet mode commands` for available commands
telnet <ip-address>[port #]	begins a Telnet session for the indicated Telnet host

Command	*Use*
telnet mode commands: *close* *exit* *open [target host][port #]* *send [send parameter]* *set <name><value>* *status* *toggle*	 closes the current Telnet connection to a target host closes the current Telnet session establishes a Telnet session with a target host sends special Telnet control functions to the currently connected target host sets operating parameters for the current Telnet session provides information about the current Telnet session sets operating parameters for the current Telnet session
term	displays the terminal type.
term set <terminal type>	sets the terminal type
tftp get	invokes the TFTP GET command
tftp put	invokes the TFTP PUT command
tftp session	displays TFTP session statistics
tftp session kill <session id>	terminates the active TFTP session specified by the session id
tftp stats (GUEST)	displays the current TFTP statistics
time[hours:minutes:seconds]	displays or changes current system time
trace [on/off]	enabled or disables call trace information reports
trace ipxwan [on/off]	enables or disables the IPXWAN tracing option
trace ppp [on/off]	enables or disables the tracing of ppp packets
udp conns	displays UDP connection status
udp stats	displays UDP statistics
ver (GUEST)	displays current software version and hardware resource revision information
wan stats	displays current WAN connection information
wr	writes current system messages to disk
ws	writes current system statistics to disk

CAUSE CODES TABLE

The following table provides Q.931 cause codes and their corresponding meanings. Cause codes may appear in Call Trace Messages.

Dec Value	*Hex Value*	*Q.931 Cause*
0	0	valid cause code not yet received
1	1	unallocated (unassigned number) Indicates that, although the ISDN number was presented in a valid format, it is not currently assigned to any destination equipment.
2	2	no route to specified transit network (WAN) Indicates that the ISDN exchange was asked to route the call through an intermediate network that is unrecognized.
3	3	no route to destination Indicates that the call was actually routed through a network that does not serve the destination address.
4	4	send special information tone
5	5	misdialed trunk prefix
6	6	channel unacceptable Indicates that the quality of service provided by the specified channel was insufficient to accept the connection.
7	7	call awarded and being delivered in an established channel Indicates that the device has been awarded an incoming call and that the call is being connected to a channel that has already been established for similar calls.
8	8	prefix 0 dialed but not allowed
9	9	prefix 1 dialed but not allowed
10	A	prefix 1 dialed but not required
11	B	more digits received than allowed, call is proceeding
16	10	normal call clearing or normal disconnect Reports the normal clearing of a call. No action required.
17	11	device busy Indicates that the called system has acknowledged the connection request, but is unable to accept the call because the B-channels are currently in use.
18	12	no device responding Indicates that the connection could not be completed because the destination failed to respond to the call.

Dec Value	*Hex Value*	*Q.931 Cause*
19	13	no answer from device (device alerted) Indicates that the destination has responded to the connection request but has failed to complete the connection within the prescribed time. Problem at remote end.
21	15	call rejected Indicates that the destination was capable of accepting the call (was neither busy nor incompatible) but rejected the call for some reason.
22	16	number changed Indicates that the ISDN number used to set up the call is no longer assigned to any system. If an alternate address has been assigned to the called equipment, this may be returned in the diagnostic field of this message.
23	17	reverse charging rejected
24	18	call suspended
25	19	call resumed
26	1A	non-selected device clearing Indicates that the destination was capable of accepting the call (was neither busy nor incompatible) but rejected the call because it was not awarded to the device.
27	1B	destination out of order Indicates that the destination could not be reached because the interface was not functioning correctly and a signaling message could not be delivered for some reason. This may be a temporary fault but one that is expected to last a relatively long time. For example, equipment off-line.
28	1C	invalid number format (incomplete number) Indicates that the connection could not be established because the destination address was presented in an unrecognized format or because the destination address was incomplete.
29	1D	facility rejected Indicates that the facility requested by the device could not be provided by the network. This could be a subscription problem.
30	1E	response to STATUS INQUIRY Indicates that the status message was generated in direct response to the prior receipt of a status enquire message.
31	1F	normal, unspecified Reports the occurrence of a normal event when no standard cause applies. No action required.
33	21	circuit out of order

Dec Value	*Hex Value*	*Q.931 Cause*
34	22	no circuit / channel available Indicates that the connection could not be established because there was no appropriate channel available to handle the call.
35	23	destination unattainable
37	25	degraded service
38	26	network (WAN) out of order Indicates that the destination could not be reached because the network was not functioning correctly and that the condition is expected to last for a relatively long time. An immediate re-connect attempt is likely to be unsuccessful.
39	27	transit delay range cannot be achieved
40	28	throughput range cannot be achieved
41	29	temporary failure Indicates that an error has occurred because the network is not functioning correctly, but that this problem is likely to be resolved shortly.
42	2A	switching equipment congestion (network congestion) Indicates that the destination could not be reached because the network switching equipment was temporarily overloaded.
43	2B	access information discarded Indicates that the network could not provide the requested access information.
44	2C	requested circuit / channel not available Indicates that the remote equipment could not provide the requested channel for an unspecified reason. This may, or may not, be a temporary problem.
45	2D	preempted
46	2E	precedence call blocked
47	2F	resource unavailable, unspecified Indicates that the requested channel or service was unavailable for an unspecified reason. This may, or may not, be a temporary problem.
49	31	quality of service unavailable Indicates that the requested quality of service (as defined by CCITT recommendation X.213) could not be provided by the network. This may be a subscription problem.
50	32	requested facility not subscribed Indicates that the remote equipment supports the requested supplementary service but that this is available only by subscription.
51	33	reverse charging not allowed

Dec Value	*Hex Value*	*Q.931 Cause*
52	34	outgoing calls barred
53	35	outgoing calls barred within CUG
54	36	incoming calls barred
55	37	incoming calls barred within CUG
56	38	call waiting not subscribed
57	39	bearer capability not authorized Indicates that the device has requested a bearer capability that the network is able to provide, but that the device is not authorized to use. This may be a subscription fault.
58	3A	bearer capability not presently available Indicates that the network is normally able to provide the requested bearer capability, but not at the present time. This may be a temporary network problem or a subscription problem.
59	3B	device busy 1TR6
61	3E	call rejected 1TR6
63	3F	service or option not available, unspecified Indicates that the network or remote equipment was unable to provide the requested service option for an unspecified reason. This may be a subscription problem.
65	41	bearer service (or capability) not implemented Indicates that the network is not capable of providing the bearer capability requested by the device.
66	42	channel type not implemented Indicates that the network or the destination equipment does not support the requested channel type.
67	43	transit network selection not implemented
68	44	message not implemented
69	45	requested facility not implemented Indicates that the remote equipment does not support the requested supplementary service.
70	46	only restricted digital information bearer capability is available Indicates that the network is unable to provide *unrestricted* digital information bearer capability.
79	4F	service or option not implemented, unspecified Indicates that the network or remote equipment was unable to provide the requested service option for an unspecified reason. This may be a subscription problem.

Dec Value	*Hex Value*	*Q.931 Cause*
81	51	invalid call reference value Indicates that the remote equipment has received a call with a call reference that is not currently in use by the device-network interface.
82	52	identified channel does not exist Indicates that the receiving equipment has been requested to use a channel that is not activated on the interface for calls.
83	53	a suspended call exists, but this call identity does not Indicates that the network received a call resume request. The call resume request contained a Call Identity information element which indicated that it is in use for a suspended call.
84	54	call identity in use
85	55	no call suspended Indicates that the network received a call resume request when there was not a suspended call pending. This may be a transient error that will be resolved by successive retries.
86	56	call having the requested call identity has been cleared Indicates that the network received a call resume request. The call resume request contained a Call Identity information element which once indicated a suspended call; however, that suspended call was cleared either by time-out or by the remote device.
88	58	incompatible destination Indicates that an attempt was made to connect to non-ISDN equipment; for example, to an analog line.
89	59	non-existent abbreviated address entry
90	5A	remote device initiated 1 TR6
91	5B	invalid transit network specified Indicates that the ISDN exchange was asked to route the call through an intermediate network that is unrecognized.
92	5C	invalid facility parameter
93	5D	mandatory information element is missing
95	5F	invalid message unspecified Indicates that an invalid message was received and that no standard cause applies. D-channel error. If this error is returned systematically, report the occurrence to your authorized service provider.
96	60	mandatory information element is missing Indicates that the receiving equipment received a message that did not include one of the mandatory information elements. D-channel error. If this error is returned systematically, report the occurrence to your authorized service provider.

Dec Value	*Hex Value*	*Q.931 Cause*
97	61	message type non-existent or not implemented Indicates that the receiving equipment received a message that was not recognized either because the message type was invalid, or because the message type was valid but not supported. This is either a problem with the remote configuration or a problem with the local D-channel.
98	62	message not compatible with call state or message type non-existent or not implemented or wrong message Indicates that an invalid message was received and that no standard cause applies. D-channel error. If this error is returned systematically, report the occurrence to your authorized service provider.
99	63	information element nonexistent or not implement Indicates that an invalid message was received by the remote equipment that contained information elements which were not recognized. D-channel error. If this error is returned systematically, report the occurrence to your authorized service provider.
100	64	invalid information element contents Indicates that a message was received by the remote equipment that included invalid information in the information element. D-channel error.
101	65	wrong message for state (message not compatible with call state) Indicates that remote equipment received an unexpected message that did not correspond to the current state of the connection. D-channel error.
102	66	recovery on timer expiry Indicates that an error-handling (recovery) procedure has been initiated by a timer expiry. This should be a temporary problem.
103	67	mandatory information element error
111	6F	protocol error Indicates an unspecified D-channel error when no other standard cause applies.
112	70	local procedure error 1TR6
113	71	remote procedure error 1TR6
127	7F	internetworking, unspecified Indicates that an event occurred but that the network does not provide causes for the actions that it takes, therefore the precise nature of the event cannot be ascertained. This may, or may not, indicate the occurrence of an error.

Dec Value	*Hex Value*	*Q.931 Cause*
UNKNOWN		Indicates that an event occurrent but that the network does not provide causes for the actions that it takes, therefore the precise nature of the event cannot be ascertained. This may, or may not, indicate the occurrence of an error.

INDEX

Numerics

9W006 modules 25
9W007 modules 25

A

accessing the module 47
admin 48, 195
administration console
  commands 268
  connector 30
administration sessions 48
AppleTalk routing
  commands 205
  port statistics 242
  problem diagnosis 96
  statistics 238
  verification 69
  verifying initialization 69
  verifying over LAN 71
  verifying over WAN 71
atalk commands 205
atalk port stats 242
atalk stats 238

B

bandwidth 18
  bandwidth reservation 73
B-channel 221
br stat 210
br stp commands 225
BRI initialization message 54
bridging
  operation verification 55
  problem diagnosis (initialization) 76, 107
  statistics 243

C

cabling 44
  Ethernet 45
  mod-tap adapter 45
call commands 210
call restrictions
  statistics 237
call statistics 237
call trace messages 168, 273
Carbon Copy 188
cause codes table 273
CFGEDIT 37
cfgedit 37
cls 39, 196
cmp commands 214
commands
  administration services 195
  AppleTalk 205
  bridging 209
  call control 210
  call restriction 213
  compression 214
  digital modem 214
  IP routing 215
  IPX 219
  ISDN usage 221
  LAN 222
  operational information 196
  packet capture 222
  set date and time 203
  SNMP 225
  spanning tree 225
  summary 268
  TCP 228
  Telnet 228
  terminal 231
  terminating and restarting 203, 204
  TFTP 232
  throughput 200
  trace 233
  UDP 234
  WAN 234
commit 39
compliance notices 3
compression 18
  operation verification 73
  problem diagnosis 107
  statistics 243
configuration
  files 32
  restoring 264
  tools
    CFGEDIT 37
    dynamic management 38
    SFVRA-CFG 36
connections table 199
connectivity statistics 236
connectors and ports 30
console connections
  using telnet 49
Console Information Port (CIP), refers to RS232 port

cr stats 213
cs 196
CSU 41
custom information 264

D
date 203
decompression statistics 244
dedicated connections
operation verification 56
problem diagnosis 80
default IP address 47
dial out 19
problem diagnosis 105
verification 73
digital modem 19
disc device 212
DOC notice 4
dr 33, 197
ds 33, 197, 236

E
er 202
error messages 110
es 202
Ethernet activity LEDs 29
Ethernet cabling 45
Ethernet ports 30
exit 196
external floppy drive connector 30

F
FCC notice 3
features 18

G
guest 195

H
hardware
available configurations 25
installation 43
overview 25
verification 53
help 39, 196
hunt group 41

I
ICMP group statistics 247
initialization messages 110
installation
hardware 43
interfaces
module 28
problem diagnosis 82
IP addresses 196
assigning of 48
default 47
ip commands 215
ip rip commands 216
ip route commands 218
IP routing
commands 215
operation verification 56
over LAN interface connection
problem diagnosis 82
verification 57
over WAN interface connection
problem diagnosis 84
verification 58
over WAN remote interface connection
problem diagnosis 86
verification 60
over WAN unnumbered interface connection
problem diagnosis 87
verification 61
problem diagnosis 76
statistics 245
verifying interfaces 57
ipconfig 48, 196
ipx commands 219
ipx route stats 252
IPX routing
commands 219
problem diagnosis 91
statistics 249
verification 66
verifying over LAN 67
verifying over remote LAN 68
verifying over WAN 68
verifying triggered RIP/SAP 69
ISDN 15
configuration options 42
ordering PRI service 41
isdn usage commands 221

K
keyboard connector 30

L
LAN adapter
initialization messages 54
problem diagnosis 75, 82
verification messages 55
lan commands 222
LAN connection
operation verification 55
LAN statistics 245
lan test 55
LEDs 28
Ethernet activity 29
power 29
SMB 29
list (file name) 197
list rel_note.txt 49
login commands 195
logout 196

M
maintenance 264
manage 38
Manage Mode 35, 38
mc 197, 200
messages
system messages 109
trace messages 168
modem commands 214
modem devices 215
Mod-Tap adapter 41, 45
module
cabling 44
illustration 27
initial access 47
interfaces 28
ports and connectors 30
restarting 46
verification 53

N
neif 197
netstat -r 64
normal operation messages 110

O
operational files 33
ordering PRI ISDN service 41

P
parallel port 30
ping 58
pkt commands 222
pkt mac 209
port statistics, AppleTalk 242
ports and connectors 30
power LED 29
PPP packet trace messages 175
PRI cabling 45
PRI ports 30
problem diagnosis
AppleTalk routing 96
bridge initialization 76
compression 107
dedicated connections 80
dial out 105
IP routing 76
IPX routing initialization 91
LAN adapter 75
RIP 88
SNMP 101
triggered RIP/SAP 95
WAN adapter 75
WAN line availability 78
pswd 48, 196

Q
quit 203

R
readme 39
regulatory compliance of platforms 28
release notes 13, 49, 51
remote device connectivity
operation verification 57
problem diagnosis 80
remote LAN
problem diagnosis 93
verification 68
remote management 179
Carbon Copy 188
SNMP 180
Telnet 182
TFTP 186
Win95 dial-up networking 185
reporting problems 266
restart 203
restarting the module 46
restoring configuration 264
RIP (IP)
commands 216
operation verification 62
problem diagnosis 88
verifying initialization 62

verifying LAN input processing 64
verifying LAN output processing 62
verifying WAN input processing 66
verifying WAN output processing 65
RS232 console connector 30

S
semipermanent connections
commands 198
verification 74
session 204
SFVRA-CFG 35, 36
features not supported by 35
starting 36
SMB LEDs 29
SMB-1 31
SNMP 180
operation verification 72
problem diagnosis 101
remote management 180
statistics 255
snmp stats 225
software
configuration files 32
operational files 33
overview 32
system files 32
upgrading 50
sp 198
Spanning Tree
bridge information 226
messages 110
port information 226
start_ne 203
statistics
AppleTalk routing 238
bridging 243
call restriction 237
call statistics 237
compression 243
connectivity 236
IP 245
IPX 249
IPX route 252
LAN 245
SNMP 255
TCP 257
TFTP 258
throughput monitoring 237
triggered RIP/SAP 251, 253
UDP 260
writing to disk 34
status 199
swapability 19
switches 24
system files 32
system management bus (SMB-1) 31
system messages
error messages 110
informational messages 109
initialization messages 110
normal operation messages 110
operational files 33
Spanning Tree messages 110
summary 110
warning messages 110
writing to disk 34
system software 32

T
TCP
statistics 257
tcp commands 228
Telco interfaces 16
Telnet 49, 182
connections 50
for module access 47
for remote access 49
remote management 182
telnet commands 229
term commands 231
term set 57
terminal application 47
TFTP 186
remote management 186
statistics 258
tftp commands 232
throughput monitor
statistics 237
time 199, 203
tools
for configuration 35
for remote management 179
trace commands 233
trace messages 168
call trace messages 168
PPP packet 175
summary 169
triggered RIP/SAP
commands 221
problem diagnosis 95
statistics 251, 253
verification 69

U

UDP
    statistics 260
udp commands 234
upgrade.osw 51
upgrading software 50, 264
utility commands 39

V

VCCI notice 4
ver 199
verification
    module installation 53
    requirements 53
verifying the installation
    AppleTalk 69
    bridge initialized 55
    compression 73
    dedicated connection 56
    dial out 73
    hardware resources 53
    IP router initialized 56
    IP routing over interfaces 57
    IPX routing 66
    LAN connection 55
    remote device connectivity 57
    reserved bandwidth 73
    RIP 62
    semipermanent connections 74
    SNMP 72
    triggered RIP/SAP 69
    WAN lines 54
VGA video port 30

W

wan 234
WAN adapter
    initialization messages 53
    line problem diagnosis 78
    problem diagnosis 75
WAN IP interface
    verification 58
WAN lines
    operation verification 54
wan stats 200
warning messages 110
WIN95 dial-up networking 185
wr 33, 202
ws 33, 202